Matrix reduction and Lagrangian submodules

O. Albouy

Matrix reduction and Lagrangian submodules

Olivier Albouy[1,2,3]

[1] Université de Lyon, F-69622, Lyon, France
[2] Université Lyon 1, Villeurbanne
[3] CNRS/IN2P3, UMR5822, Institut de Physique Nucléaire de Lyon

E-mail: o.albouy@ipnl.in2p3.fr

Abstract

This paper deals with three technical ingredients of geometry for quantum information. Firstly, we give an algorithm to obtain diagonal basis matrices for submodules of the $\mathbb{Z}_d$-module $\mathbb{Z}_d^n$ and we describe the suitable computational basis. This algorithm is set along with the mathematical properties and tools that are needed for symplectic diagonalisation. Secondly, with only symplectic computational bases allowed, we get an explicit description of the Lagrangian submodules of $\mathbb{Z}_d^{2n}$. Thirdly, we introduce the notion of a fringe of a Gram matrix and provide an explicit algorithm using it in order to obtain a diagonal basis matrix with respect to a symplectic computational basis whenever possible. If it is possible, we call the corresponding submodule nearly symplectic. We also give an algebraic property in order to single out symplectic submodules from nearly symplectic ones.

PACS numbers: 03.65.Fd, 02.10.Yn, 03.67.-a
Keywords: finite quantum mechanics - finitely generated modules - symplectic product - matrix reduction - Lagrangian submodules - Gram matrix - nearly symplectic submodules

Introduction

In recent years, quantum information has grown with increasing interest and speed. The widest known stimulation for that is the hope of a much more efficient treatment of information with nanocircuits on the one hand and quantum algorithms on the other hand. All this is thought to be achievable, both theoretically and practically, by exploiting the main features of quantum physics, namely state superposition and entanglement. Let us be more specific as to quantum algorithms. There have been but a few of them available till now, but as shown for instance by the Bennett and Brassard's algorithm BB84 [1] and its generalisations for secure communication or on the contrary the Shor's algorithm [2] the realisation of which would break the widespread RSA code by factorising integers in polynomial time, they often rely on the discrete Fourier transform (DFT). This core transformation is only a particular case of another major topic in quantum theory, namely mutually unbiased bases (MUBs). The characteristic of such a set of bases is that a state picked out of one of them has equal amplitude over the states of any other one. In the matrix representing the discrete Fourier transform, every entry has the same modulus. Thus the basis one gets by means of the DFT is unbiased with the computational basis.

Besides Fourier transform, the notion of MUBs is widespread both in classical and quantum information theory. Schwinger unveiled them as soon as 1960 in a paper about unitary operators but he did not name them [3]. They appear in quantum tomography [4] and in quantum games such as the Mean King problem [5][6][7]. As to classical information theory, one finds them in the study of Kerdock codes [8] and spherical codes [9] or in the developpement of network communication protocols [10][11].

Since the beginning of their study in the 80's [12][4], we know that a set of MUBs in a d-dimensional Hilbert space contains at most $d+1$ of them and that this upper-bound can be achieved if d is power of a prime. But whenever d is a composite integer and despite an extensive range of mathematics involved, no conclusive information is available about the achievement of the upper-bound. As a nonexhaustive list of the mathematical tools that have been used, let us cite Galois fields and rings in relation with Gaussian sums [4][13][14], combinatorics, latin squares [6], unitary operator bases [3][15], discrete phase space [16][17] and Wigner functions [7][18][19], Fourier transform [20][21], finite ring geometry [22][23][24] and also $SU(n)$ Lie groups and their corresponding Lie algebras [25][26][27] with connection to positive operator-valued measures (POVMs) [28].

Several definitions of the Pauli matrix group have been given throughout these works. But any of them will be satisfactory for our purpose. Starting from a paper by Bandyopadhay *et al.* [15] and from a study of the Mermin square [29], the strain of finite geometry has addressed the issue of finitely generated modules over $\mathbb{Z}_d$. It appears as a useful, arithmetical translation of the behaviour of the Pauli operators. The Pauli group divided by its center group is isomorphic to a $\mathbb{Z}_d$-module and by the same token, a tensor product of Pauli groups gives rise to the direct sum of the corresponding $\mathbb{Z}_d$-modules. Despite this isomorphism is related to a quotient group, commutation relations among the Pauli operators themselves and their ability to yield MUBs can be translated as geometrical features in the $\mathbb{Z}_d$-module we have just mentioned. In particular, the symplectic inner product, Lagrangian submodules and projective nets appeared to be the objects of interest. About the connection between MUBs and Lagrangian submodules, the Heisenberg group and nice error bases, see [30] and [31]. The first of those two papers takes place in the frame of Galois fields. The use of projective lines is illustrated in [32][33] and other references therein, and their study in relation with their underlying $\mathbb{Z}_d$-module is started in [34][35]. Moreover, the action of the Clifford group over a given Pauli group has its own geometrical counterpart in the $\mathbb{Z}_d$-module and can be studied as such.

In this paper, we give a set of tools in order to delve into the structure of the submodules one meets in quantum theory. Thus in Section 1 we deal with basic manipulations of matrices over $\mathbb{Z}_d$ and simple diagonalisation. Note that the reduction in question is that of matrices whose column vectors form a basis of a given submodule, not of matrices representing linear maps. The properties and tools we introduce in that section are then used in the frame of symplectic reduction. In Section 2, we build an algorithm in order to reduce basis matrices to a particular form using only symplectic changes of basis. This algorithm enables us to set a description of the Lagrangian submodules of $\mathbb{Z}_d^{2n}$ in Section 3. Finally, the issue of symplectic diagonalisation is completed for its own sake in Section 4.

This paper is primarily intended to physicists and computer scientists coming to quantum information with various backgrounds. The mathematical tools involved are all elementary. However, to make the paper self-contained, we recall every feature of interest for our particular purpose in two appendices.

1 Simple reduction

Let d be any integer ≥ 2. For any specific notations, the reader is referred to the appendices. As is the case for vector space theory over a field, vectors in finitely generated modules and linear maps between such modules can be represented by matrices. The canonical computational basis for vectors will be denoted e. A $k \times l$ matrix m is upper-triangular (resp. lower-triangular) if for all $i \in \{1, \ldots, k\}$, $j \in \{1, \ldots, l\}$, $i > j$ (resp. $i < j$), we have $m_{ij} = 0$. The matrix m is diagonal if for all $i \in \{1, \ldots, k\}$, $j \in \{1, \ldots, l\}$, $i \neq j$, we have $m_{ij} = 0$. The m_{ii}'s of any matrix will be called its diagonal coefficients. We extend to matrices the factor projections π_p defined in the Chinese remainder theorem (see Appendix A.2): If m is a $k \times l$ matrix over $\mathbb{Z}/d\mathbb{Z}$ and p is a prime factor of d, then $\pi_p(m)$ is the $k \times l$ matrix over $\mathbb{Z}/p^s\mathbb{Z}$, $s = v_p(d)$, whose (i, j) coefficient is $\pi_p(m_{ij})$. Also p-valuation is extended to matrices:

$$v_p(m) = \min(v_p(m_{ij}); i \in \{1, \ldots, k\}, j \in \{1, \ldots, l\}). \tag{1}$$

Throughout the paper, we will adopt the conventions that a $*$ in a matrix denotes an arbitrary or unknown coefficient or submatrix, and a blank denotes a null coefficient or submatrix. The $k \times k$ indentity matrix will be written I_k and the $k \times l$ null matrix $0_{k,l}$ if necessary.

In this section and the next one, we address trigonalisation and diagonalisation of matrices whose columns are basis vectors of a submodule of $\mathbb{Z}_d^n$. A left-multiplication by an invertible matrix is to be interpreted either as an active transformation, that is to say an automorphism of $\mathbb{Z}_d^n$, or as a passive transformation, that is to say a change of computational (free) basis. A right-multiplication by an invertible matrix stands for a change of basis of the submodule under consideration. The structure of the given submodule will be much easier to study after reduction. The reader interested in a more abstract treatment of simple reduction and in particular diagonalisation of matrices over more general rings may have a look to [36][37][38]. By the way, we shall also have an insight into generalisation over $\mathbb{Z}_d$ of the "Incomplete basis theorem". The set of invertible matrices over $\mathbb{Z}$ is denoted $\mathrm{GL}(n, \mathbb{Z})$ and the set of invertible matrices over $\mathbb{Z}_d$ is denoted $\mathrm{GL}(n, \mathbb{Z}_d)$. Note that left-multiplication by an invertible matrix does not modify the order of a column vector and hence does not modify the gcd of its coefficients. The same is true for right-multiplication and row-vectors.

The only preliminary result we shall admit is that a square matrix with coefficients in a commutative ring is invertible iff its determinant is an invertible element of that ring (see [36]). In fact, the proof is a mere copy of the field case.

Before we go on, a general remark is in order about the algorithms presented in this paper. Except the algorithm $\mathscr{D}_\omega$ for symplectic diagonalisation, they are "blind" algorithms, that is to say we do not suppose we know where invertible coefficients are located in the matrices, what would be mandatory to use the classical Gaussian reduction for instance.

Lemma 1 *Let $a \in \mathbb{Z}_d^n$ be an n-dimensional vector. Then*

$$\exists L \in \mathrm{GL}(n, \mathbb{Z}_d), \exists k \in \mathbb{Z}_d, La = ke_1. \tag{2}$$

The column vectors $C_1, \dots, C_n$ of L^{-1} form a free basis of $\mathbb{Z}_d^n$ such that $kC_1 = a$.

Proof. Our calculations to prove this lemma will be in $\mathbb{Z}$. The results will only have to be sent onto residue classes at the end. Let $a \in \mathbb{Z}^n$, $\delta_{n-1} = a_{n-1} \wedge a_n$, $a'_{n-1} = a_{n-1}/\delta$, $a'_n = a_n/\delta$. There exist $k_1, l_1 \in \mathbb{Z}$ such that $k_1 a_{n-1} + l_1 a_n = \delta_{n-1}$ so that we have the active transformation on a:

$$\underbrace{\left(\begin{array}{c|cc} I_{n-2} & & \\ \hline & k_1 & l_1 \\ & -a'_n & a'_{n-1} \end{array}\right)}_{L^{(n-1)} \in \mathrm{GL}(n,\mathbb{Z})} \underbrace{\left(\begin{array}{c} * \\ \hline a_{n-1} \\ a_n \end{array}\right)}_{a} = \underbrace{\left(\begin{array}{c} * \\ \hline \delta_{n-1} \\ 0 \end{array}\right)}_{a^{(n-1)}}. \tag{3}$$

Repeating this trick on $a^{(n-1)}$ with components $n-1$ and $n-2$ and so on, we bring the vector a onto a multiple of e_1. Of course, the order of k in $\mathbb{Z}_d$ is the same as the order of a in $\mathbb{Z}_d^n$. In details:

$a^{(n)} = a, \delta_n = a_n,$

$$\forall i \in \{1, \dots, n-1\}, \left\{\begin{array}{rcl} \delta_{n-i} & = & a_{n-i} \wedge \delta_{n-i+1} \\ a'_{n-i} & = & a_{n-i}/\delta_{n-i} \\ \delta'_{n-i+1} & = & \delta_{n-i+1}/\delta_{n-i} \\ \multicolumn{3}{c}{\exists k_i, l_i \in \mathbb{Z}_d, k_i a_{n-i} + l_i \delta_{n-i+1} = \delta_{n-i}} \end{array}\right. ,$$

$$\underbrace{\left(\begin{array}{c|cc|c} I_{n-i-1} & & & \\ \hline & k_i & l_i & \\ & -\delta'_{n-i+1} & a'_{n-i} & \\ \hline & & & I_{i-1} \end{array}\right)}_{L^{(n-i)}} \underbrace{\left(\begin{array}{c} * \\ \hline a_{n-i} \\ \delta_{n-i+1} \\ \hline 0_{i-1,1} \end{array}\right)}_{a^{(n-i+1)}} = \underbrace{\left(\begin{array}{c} * \\ \hline \delta_{n-i} \\ 0 \\ \hline 0_{i-1,1} \end{array}\right)}_{a^{(n-i)}}. \tag{4}$$

Each $L^{(i)}$ has determinant 1, so that the complete transformation given by the product $L = \prod_{i=1}^{n-1} L^{(i)}$ also has and therefore is an automorphism. So we have shown what we were seeking for:

$$\exists L \in \mathrm{GL}(n, \mathbb{Z}), \exists k \in \mathbb{Z}, La = ke_1. \tag{5}$$

■

Lemma 2 *Let $a_1, a_2 \in \mathbb{Z}_d^n$ of order ν_1, ν_2 respectively. There exists a linear combination a of a_1, a_2 of order $\nu_1 \vee \nu_2$. Moreover, if d is odd, we can build a such that*

$$\langle a, a_1 \rangle = \langle a, a_2 \rangle = \langle a_1, a_2 \rangle . \tag{6}$$

If d is even, then in general we can have only

$$\langle a, a_1 \rangle \ \ or \ \langle a, a_2 \rangle = \langle a_1, a_2 \rangle . \tag{7}$$

Proof. If a_1 or a_2 is equal to 0, the lemma is obvious. We now suppose that they are not and that d is odd. Let $A = (a_1|a_2)$ be the $n \times 2$ matrix whose columns are a_1, a_2 and with the help of lemma 1, left-multiply A by an invertible matrix L such that La_1 has all but its first coefficient equal to 0. The matrix L is to be interpreted as a change of basis. If $k_1, \ldots, k_n$ are the coefficients of the second column of LA, let $\delta = k \wedge k_1$. According to lemma 13 of Appendix A.2, there exist $u, v \in U(\mathbb{Z}_d)$ such that

$$\delta = uk + vk_1. \tag{8}$$

Then we put

$$(a_1'|a) = LA \begin{pmatrix} 0 & u \\ -u^{-1} & v \end{pmatrix} \text{ and } (a|a_2') = LA \begin{pmatrix} u & 0 \\ v & u^{-1} \end{pmatrix}. \tag{9}$$

or

$$(a_1'|a) = LA \begin{pmatrix} v^{-1} & u \\ 0 & v \end{pmatrix} \text{ and } (a|a_2') = LA \begin{pmatrix} u & -v^{-1} \\ v & 0 \end{pmatrix}. \tag{10}$$

In any case, a answers the lemma since, with lemma 12 and equations (117), (128a) and (141) of the appendices, the order of a is

$$\begin{aligned} \nu(a) = \frac{d}{\delta \wedge (\bigwedge_{i=2}^n k_i) \wedge d} &= \frac{d}{(k \wedge d) \wedge (\bigwedge_{i=1}^n k_i \wedge d)} \\ &= \left(\frac{d}{k \wedge d} \right) \vee \left(\frac{d}{\bigwedge_{i=1}^n k_i \wedge d} \right) = \nu(a_1) \vee \nu(a_2). \end{aligned} \tag{11}$$

And for $i = 1, 2$,

$$\langle a, a_i \rangle = \langle a, a_i' \rangle = \langle a_1, a_2 \rangle . \tag{12}$$

To complete the proof, let us deal with the case where $d = 2^s$. With $i = 1$ or 2 such that $\nu(a_i) = \min(\nu(a_1), \nu(a_2))$, we simply put $a = a_i$. ■

Note that for any linear combination $b = b_1 a_1 + b_2 a_2$ of a_1 and a_2,

$$\nu(a) b = b_1(\nu(a) a_1) + b_2(\nu(a) a_2) = 0. \tag{13}$$

Thus for all $b \in \langle a_1, a_2 \rangle$, $\nu(b)$ divides $\nu(a)$.

Given two minimal bases $f = (f_1, \ldots, f_r)$ and $g = (g_1, \ldots, g_r)$ of a submodule M, it is in general not possible to find an automorphism of M that brings f_i onto g_i for all i, even if $\nu(f_i) = \nu(g_i)$ for all i. Indeed in $\mathbb{Z}_6$, we cannot find $a \in \mathbb{Z}_6$ and $b \in U(\mathbb{Z}_6)$ so that

$$\begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix}. \tag{14}$$

We can take b to be 1 or 5. But a should be such that $1+3a=2$, what is impossible. As to diagonalisation, left-multiplication is still not sufficient, especially because the order of respective column vectors from one basis to the other is not preserved:

$$\begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 3 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}. \tag{15}$$

We shall make use of lemma 2 to perform diagonalisation with left- and right-multiplications. For instance, the latter inequation is solved trivially:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 3 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}. \tag{16}$$

Suppose that we are given a minimal basis $b=(b_1,\dots,b_r)$ of a submodule M of $\mathbb{Z}_d^n$ and B is the matrix of size $n\times r$ whose i-th column is b_i. The matrix B is called a basis matrix for M. With the help of lemma 1, we could easily put B in an upper-triangular form by means of left-multiplications. But we are going to transform it into a new, diagonal matrix whose column vectors still generate M. Because of lemma 2 and associativity of lcm, we may suppose that

$$\nu(b_1) = \bigvee_{i=1}^{r} \nu(b_i), \tag{17a}$$

$$\forall m \in M, \nu(m)|\nu(b_1). \tag{17b}$$

An algorithm which set any matrix that way will be called $\mathscr{A}$. It consists of an appropriate right-multiplication by an invertible matrix. We left-multiply B by a matrix L_1 with determinant 1 so that $L_1 b_1$ has all but its first coefficient equal to 0. Let $\widetilde{B}=L_1 B$. If one of the coefficients of $\widetilde{B}$ but in the first column, say $\widetilde{b}_{ij}$, $j\geq 2$, were not a multiple of the upper-left coefficient $\widetilde{b}_{11}$, then $\nu\left(\widetilde{b}_{ij}\right)$ would not be a divisor of $\nu\left(\widetilde{b}_{11}\right)=\nu(b_1)$ and according to relation (140) of Appendix B and to lemma 2 again, there would exist a linear combination of b_1 and b_j of order greater than $\nu(b_1)$, what is impossible by assumption. Since we are only interested in a basis of M we can put all but the first coefficient of the first row to 0 and obtain a matrix B_1. This is equivalent to a right-multiplication by an appropriate invertible matrix. Carrying on this process, we obtain a diagonal matrix B_r whose column vectors still form a minimal basis of M. Let us describe the algorithm in details.

Algorihtm $\mathscr{D}_0$: The starting point is the empty matrix D_0 with no lines and no columns, and as an argument a $k\times l$ matrix B. Let $B_0=B$. Then for i from 0 to $\mu=\min(k-1,l-1)$, we go on the following steps:

1. $R_{i+1}^{(1)} = \begin{pmatrix} I_i & 0 \\ 0 & R' \end{pmatrix}$ with R' a $(l-i)\times(l-i)$ invertible matrix such that $\mathscr{A}(B_i)=B_i R'$.

2. $L_{i+1} = \begin{pmatrix} I_i & 0 \\ 0 & L' \end{pmatrix}$ with L' an $(k-i)\times(k-i)$, determinant-1 matrix given by lemma 1 such that $B'=L'\mathscr{A}(B_i)$ has all its first column coefficients but the first one equal to 0.

3. $R^{(2)}_{i+1} = \begin{pmatrix} I_i & 0 \\ 0 & R'' \end{pmatrix}$ with R'' a $(l-i) \times (l-i)$ invertible matrix such that $B'R''$ has all its first line coefficients but the first one equal to 0.

4. $D_{i+1} = \begin{pmatrix} D_i & 0 \\ 0 & b'_{11} \end{pmatrix}$.

5. B_{i+1} is given from B' by deleting the first row and the first column of this latter one.

The results of the algorithm are the change of basis matrices $L(B) = \prod_{i=1}^{\mu+1} L_{\mu+2-i}$, $R(B) = \prod_{i=1}^{\mu+1} R^{(1)}_i R^{(2)}_i$ and the $k \times l$ diagonal matrix $\mathscr{D}_0(B)$ defined to be

$$\begin{pmatrix} D_{\mu+1} \\ 0_{k-l,l} \end{pmatrix} \text{ or } \begin{pmatrix} D_{\mu+1} & 0_{k,l-k} \end{pmatrix} \tag{18}$$

whether $k \geq l$ or $k \leq l$ respectively. For all $i, j \in \{1, \ldots, r\}$, $i < j$, we have $(D_{\mu+1})_{ii} | (D_{\mu+1})_{jj}$. ♦

As to the minimal basis b, the second case for $\mathscr{D}_0(B)$ is impossible and thus $r \leq n$. The minimality of b also implies that none of the diagonal coefficients of $D_{\mu+1} = D_r$ is 0. Hence, the column vectors of $\mathscr{D}_0(B)$ still form a minimal basis of M. Additionally, note that if we replace every diagonal entry of $\mathscr{D}_0(B)$ by 1, the column vectors of the matrix we obtain form a free basis $\widehat{b}$ of a free, rank-r submodule $M_{\widehat{b}}$ containing M.

The remaining features stated in theorem 3 below are immediate consequences of the classification of finite, commutative groups. However, we are to prove them as an illustration of our topic which is reduction of matrices with coefficients in $\mathbb{Z}_d$.

If we start with a nonminimal basis of M, say b' with $r + r'$ vectors, $r' \geq 1$, the algorithm $\mathscr{D}_0$ yields a matrix of the form

$$\mathscr{D}_0(B') = \begin{pmatrix} D & 0_{n,r+r'-k} \end{pmatrix}, \tag{19}$$

where D is a diagonal matrix with k columns, all of them nonzero. Since M is of rank r, we have $k \geq r$. Suppose $k > r$ and let $\widetilde{D}$ be the $(1, \ldots, n; 1, \ldots, r+1)$ submatrix of D. There exists an $r \times (r+1)$ matrix E whose j-th column, $j \in \{1, \ldots, r+1\}$, contains the components of the j-th column vector of $\widetilde{D}$ with respect to the free basis $\widehat{b}$. A linear combination of the column vectors of $\widetilde{D}$ with some factors is null iff the linear combination of the respective column vectors of E with these same factors is null. In other words, $\widetilde{D}$ and E have the same kernel as linear maps. Applying the algorithm $\mathscr{D}_0$ to E, we construct a null linear combination of its column vectors the factors of which are located in the last column C of $R(E)$. Now, let us choose a prime factor p of d such that $t = v_p(d_{r+1,r+1}) < v_p(d)$, so that no diagonal entry of $\pi_p(\widetilde{D})$ is null. There exists such a p because $d_{r+1,r+1} \neq 0$. Since $R(E)$ is invertible, at least one of the factors contained in $\pi_p(C)$ is a unit. But in that case, $\pi_p(\widetilde{D}C)$ cannot be null as expected. So $k = r$. Thus we may add to the algorithm $\mathscr{D}_0$ a final step to get the

Simple reduction algorithm $\mathscr{D}$: Let M be a rank-r submodule of $\mathbb{Z}_d^n$, b a basis of M containing $s \geq r$ vectors and B the corresponding basis matrix. By deleting the last $s-r$ null columns of $\mathscr{D}_0(B)$, one gets a minimal basis matrix for M. The matrix $\mathscr{D}(b)=\mathscr{D}(B)$ thus obtained is called the simple reduction of the basis b or of the basis matrix B. ⧫

Let $b^{(1)}$ and $b^{(2)}$ be two bases of M. In the next three paragraphs, we are going to work in a single Chinese factor, say with prime factor p, and we are to prove that for every $i\in\{1,\dots,r\}$, the i-th diagonal entries of $\mathscr{D}(b^{(1)})$ and $\mathscr{D}(b^{(2)})$ are associated. In order to make notations lighter, we even suppose that d is a power of a prime, say p^s. There is a slight difference, since in the latter case, r may vary with the Chinese factor one chose initially. The reader may check that such a trick is allowed. Let $B^{(a)}=L(b^{(a)})^{-1}\mathscr{D}(b^{(a)})$, $a\in\{1,2\}$, $\widehat{B}$ be the representative matrix of $\widehat{b}$ with respect to the computational basis and P^{12}, P^{21} and E be three $r\times r$ matrices such that

$$B^{(1)}P^{12}=B^{(2)},\quad B^{(2)}P^{21}=B^{(1)},\quad \widehat{B}E=B^{(1)}. \tag{20}$$

So we have

$$\widehat{B}EP^{12}P^{21}=B^{(1)}P^{12}P^{21}=B^{(1)}=\widehat{B}E \tag{21}$$

and then

$$\mathscr{D}(E)P=\mathscr{D}(E),\ \text{with } P=R(E)^{-1}P^{12}P^{21}R(E). \tag{22}$$

If some diagonal entry of $\mathscr{D}(E)$ were zero, then the column vectors of $B^{(1)}R(E)=\widehat{B}L(E)^{-1}\mathscr{D}(E)$ would form a basis of M with at most $r-1$ elements, what is impossible. So there exists an $r\times r$ matrix Q such that $P=I_r+pQ$. Hence P is invertible, and so are P^{12} and P^{21}. For $a\in\{1,2\}$, consider the maps

$$\begin{array}{rrcl} f^{(a)}: & (\mathbb{Z}/p^s\mathbb{Z})^r & \longrightarrow & M \\ & X & \longmapsto & B^{(a)}X \end{array} \tag{23}$$

where elements of $(\mathbb{Z}/p^s\mathbb{Z})^r$ are presented as column vectors and let $n_i^{(a)}$, $i\in\{0,\dots,s\}$, be the number of vectors X so that $f^{(a)}(X)$ is of order p^{s-i}. For every X so that $B^{(1)}X$ is of order p^{s-i}, the vector $Y=P^{21}X$ is so that $B^{(2)}Y$ is of order p^{s-i} as well. Since P^{21} is injective as a linear map, we have $n_i^{(2)}\geq n_i^{(1)}$. The converse inequality can be shown the same way and so $n_i^{(1)}=n_i^{(2)}$.

Now let b be any basis of M and r_i, $i\in\{0,\dots,s\}$, be the number of diagonal entries of $D=\mathscr{D}(b)$ of the form up^i, $u\in U(\mathbb{Z}/p^s\mathbb{Z})$. We also define the following two related objects

$$\forall i\in\{-1,\dots,s-1\},\sigma_i=\sum_{j=0}^{i}r_j, \tag{24}$$

and as intervals in $\mathbb{N}$

$$\forall i\in\{0,\dots,s-1\},K_i=\{\sigma_{i-1}+1,\dots,\sigma_i\}. \tag{25}$$

The cardinality of a K_i is of course r_i. We are to prove by induction on i that the r_i's do not depend on the choice of b and so are properties of M. As in the previous paragraph, consider the map

$$\begin{array}{rrcl} f: & (\mathbb{Z}/p^s\mathbb{Z})^r & \longrightarrow & M \\ & X & \longmapsto & DX. \end{array} \tag{26}$$

The number of vectors X so that $f(X)$ is of order p^{s-i}, $i \in \{0, \dots, s-1\}$, is

$$n_i = \sum_{j=0}^{i} \left\{ \left[\prod_{k=0}^{j-1} p^{((s-1)-(i-k))r_k} \right] \times \left[p^{((s-1)-(i-j-1))r_j} - p^{((s-1)-(i-j))r_j} \right] \times \right.$$
$$\left. \times \left[\prod_{k=j+1}^{i} p^{((s-1)-(i-k-1))r_k} \right] \right\} \times \prod_{l=i+1}^{s-1} p^{sr_l}. \quad (27)$$

Indeed, one can consider the bar graph in figure 1 to see where that latter expression comes from.

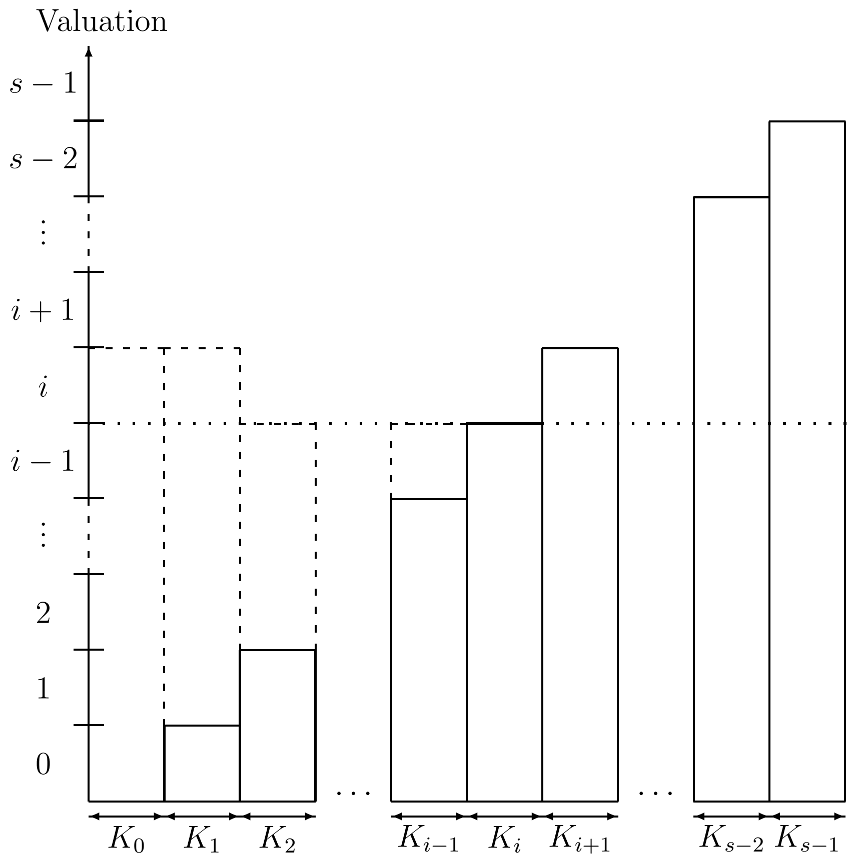

Figure 1: How to calculate the n_i's

The individual positions on the horizontal axis have not been displayed. Instead, only the relevant intervals of them have been. For any $X \in (\mathbb{Z}/p^s\mathbb{Z})^r$ and any $a \in \{0, \dots, r\}$, the vertical bars in plain or dashed lines and the horizontal dotted line above the a-th position show lower bounds for the p-valuation of the a-th coefficient of $f(X)$. Thus as a property of D, if $a \in K_l$, we have $v_p(f(X)_a) \geq l$ as shown by the plain line bars. Since the order of $f(X)$ is prescribed to be p^{s-i}, $v_p(f(X)_a) \geq i$ as shown by the dotted line. Finally, we put

$$j = \min(k \in \{0, \dots, s\}; \exists l \in K_k, v_p(f(X)_l) = i). \quad (28)$$

There exists such a j ($j = 2$ in the example on the graph) and if $a \leq j-1$, $v_p(f(X)_a) > i$ as shown by the dashed line bars. These various lower bounds partition $\{0,\ldots,r\}$ into four subintervals corresponding to the four factors in the above expression of n_i. The sum amounts for all the possibilties for j.

For $i = 0$, we have

$$n_0 = (p^{sr_0} - p^{(s-1)r_0})p^{s(r-r_0)} = p^{sr}\left(1 - \frac{1}{p^{r_0}}\right). \tag{29}$$

This quantity, which is a property of M, would increase strictly with r_0. Hence r_0 does not depend on the choice of b. For $i \geq 1$, we suppose that for $j \leq i-1$, the r_j's do not depend on b. Then there exist a nonnegative integer α and a positive integer β such that

$$n_i = (\alpha p^{sr_i} + \beta(p^{sr_i} - p^{(s-1)r_i}))p^{s(r-\sigma_{i-1}-r_i)} = p^{s(r-\sigma_{i-1})}\left(\alpha + \beta - \frac{\beta}{p^{r_i}}\right). \tag{30}$$

Again, we conclude that r_i does not depend on b. The number n'_i of vectors of order p^{s-i} in M, $i \in \{0,\ldots,s\}$, would have been much more obvious a property of M. But for $i \in \{0,\ldots,s-1\}$:

$$\begin{aligned} n'_i = \sum_{j=0}^{i}\Bigg\{\left[\prod_{k=0}^{j-1} p^{((s-k-1)-(i-k))r_k}\right] \times \left[p^{((s-j-1)-(i-j-1))r_j} - p^{((s-j-1)-(i-j))r_j}\right] \times \\ \times \left[\prod_{k=j+1}^{i} p^{((s-k-1)-(i-k-1))r_k}\right]\Bigg\} \times \prod_{k=i+1}^{s-1} p^{((s-k-1)-(-1))r_k} \\ = \sum_{j=0}^{i}\Bigg\{\left[\prod_{k=0}^{j-1} p^{(s-i-1)r_k}\right] \times \left[p^{(s-i)r_j} - p^{(s-i-1)r_j}\right] \times \left[\prod_{k=j+1}^{i} p^{(s-i)r_k}\right]\Bigg\} \times \prod_{k=i+1}^{s-1} p^{(s-k)r_k}, \end{aligned} \tag{31}$$

with a cumbersome $\sum_{k=i+1}^{s-1} kr_k$ appearing as an exponent in the last factor. Even if we looked at n'_i/n'_{i-1} to handle the induction, that exponent would stay for the initialisation at $i = 0$.

Finally, harking back to the case where d is not necessarily a power of a prime, the number $r_s = r - (r_0 + \ldots + r_{s-1})$ of diagonal entries of $\mathscr{D}(b)$ with p-valuation $v_p(d)$ is a property of M. We sum up our results about simple reduction in the

Theorem 3 *For any rank-r submodule M of $\mathbb{Z}_d^n$, there exist a free basis f of $\mathbb{Z}_d^n$ and a minimal basis b of M such that:*

1. *b is represented by a diagonal $n \times r$ matrix B with respect to f;*
2. *for all $i, j \in \{1,\ldots,r\}$, $i < j$, we have $b_{ii}|b_{jj}$.*

Such a pair of bases (f, b) can be found from any basis b_0 of M by the simple reduction algorithm $\mathscr{D}$. Moreover, for any pair (f, b) as above, the sequence $(d/\nu(b_{ii}))_{i\in\{1,\ldots,r\}}$ of the diagonal entries of B "without unit factors" is the same and therefore is a property of M. We shall call it the characteristic sequence of M.

With the notations of the theorem, M is free iff for all $i \in \{1, \dots, r\}$, b_{ii} is a unit in $\mathbb{Z}_d$, or in other words iff its characteristic sequence contains only 1's.

Corollary 4 *Let $\beta_0 = (b_1, \dots, b_r)$ be a free family of $\mathbb{Z}_d^n$. Then $r \leq n$ and there exist $n - r$ vectors $b_{r+1}, \dots, b_n \in \mathbb{Z}_d^n$ so that $\beta = (b_1, \dots, b_r, b_{r+1}, \dots, b_n)$ is a free basis of $\mathbb{Z}_d^n$.*

Proof. Indeed, with D the $(1, \dots, r; 1, \dots, r)$ submatrix of the $r \times n$ diagonal matrix $\mathscr{D}(\beta_0)$, a representative matrix for such a β with respect to the computational basis is

$$L(\beta_0)^{-1} \operatorname{diag}(DR(\beta_0)^{-1}, I_{n-r}). \tag{32}$$

■

Corollary 5 *For any two submodules M and N of $\mathbb{Z}_d^n$ with the same characteristic sequence, what implies that they have the same rank, there exists an automorphism of $\mathbb{Z}_d^n$ that brings M onto N.*

Proof. Let (f, b) (resp. (h, c)) be a convenient pair for M (resp. N) as in theorem 3. Then the automorphism of $\mathbb{Z}_d^n$ defined by $b_i \mapsto c_i$, $i \in \{1, \dots, n\}$, brings M onto N. ■

The pair (f, b) in theorem 3 is not unique. For the sake of Section 4, we study the relation between the various suitable bases f's. Let $(f^{(1)}, b^{(1)})$ and $(f^{(2)}, b^{(2)})$ be two convenient pairs and P the $n \times n$ change of basis matrix defined by $f^{(1)}P = f^{(2)}$. Let us work in a single Chinese factor. Let the K_i's be defined as in (25) plus

$$K_s = \{r + 1, \dots, n\}. \tag{33}$$

For any $k \in \{0, \dots, n\}$, there exists some $i_k \in \{0, \dots, s\}$ so that $k \in K_{i_k}$. So $p^{i_k} f_k^{(2)} \in M$ and hence

$$\forall i \in \{i_k + 1, \dots, s\}, \forall j \in K_i, p^{i - i_k} | P_{jk}. \tag{34}$$

Since P is invertible, we also deduce from that latter result that for any $i \in \{0, \dots, s\}$, the $(K_i; K_i)$ diagonal block of P is an invertible matrix.

As a converse, for any convenient pair (f, b) and any invertible matrix P satisfying relation (34), let b' be the family represented by the matrix $fP\mathscr{D}(b)$ and N be the submodule of M generated by b'. Since P is invertible, fP is a free family and (fP, b') is a convenient pair for N. Hence M and N have the same characteristic sequence and with the help of corollary 5, we see that they have the same cardinality. So $N = M$ and (fP, b') is a convenient pair for M.

Let $\Sigma_{\mathscr{D}}(M)$ be the subgroup of $\mathrm{GL}(n, \mathbb{Z}_d)$ that consists all the change of basis matrices we have just pointed out.

2 Symplectic reduction

In this section, we replace $\mathbb{Z}_d^n$ by $\mathbb{Z}_d^{2n}$, that is to say we take an even number of copies of $\mathbb{Z}_d$. Let $J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and ω be the canonical symplectic inner product in $\mathbb{Z}_d^{2n}$. It is defined with respect to the canonical basis by the $2n \times 2n$ block-diagonal matrix

$$J_n = \begin{pmatrix} J & & \\ & \ddots & \\ & & J \end{pmatrix}. \tag{35}$$

A basis $(b_1, \ldots, b_{2n})$ such that for all $i, j \in \{1, \ldots, n\}$, $i \neq j$,

$$\omega(b_{2i-1}, b_{2i}) = -\omega(b_{2i}, b_{2i-1}) = 1 \text{ and } \omega(b_{2i}, b_{2j-1}) = \omega(b_{2i}, b_{2j}) = 0 \tag{36}$$

is called a symplectic basis. The canonical basis is symplectic.

In simple reduction, we allowed any change of computational basis. In this section, we are interested in reduction where changes of computational basis can only be symplectic. This means that in the new basis, ω is still to be represented by J_n. Matrices L used for left-mutiplication thus have to satisfy the condition:

$$L^T J_n L = J_n, \tag{37}$$

where L^T is the transpose of L. Such a matrix is called a symplectic matrix. The identity matrix is symplectic. A matrix that represents a symplectic basis with respect to another symplectic basis is symplectic. Note that in $\mathbb{Z}$, a symplectic matrix has determinant ± 1. The same is thus true for a symplectic matrix over $\mathbb{Z}_d$. This proves that all symplectic matrices are invertible. Moreover, the inverse of a symplectic matrix is symplectic. Our plan here is the same as in the previous section. We first address reduction of a single vector and afterwards that of a matrix. The case $n = 1$ should be trivial to the reader by now. Reduction of a single vector when $n \geq 2$ relies itself on the fondamental case $n = 2$. The following substeps are elementary operations that we shall use later on in the various steps of our symplectic reduction algorithm for matrices. They form a sequence in order to reduce a vector with four components $(x, y, z, t)^T$ using only symplectic changes of basis.

Substep 1: Let $x, y, z, t \in \mathbb{Z}_d$ and $\delta = x \wedge y \wedge z \wedge t$. According to corollary 14, there exist $k_1, k_2, k_3 \in \mathbb{Z}_d$ and $u \in U(\mathbb{Z}_d)$ such that

$$\underbrace{\begin{pmatrix} u & 0 & 0 & 0 \\ k_1 & u^{-1} & k_2 & k_3 \\ -k_3 u & 0 & 1 & 0 \\ k_2 u & 0 & 0 & 1 \end{pmatrix}}_{S_1} \begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix} = \begin{pmatrix} x_1 \\ \delta \\ z_1 \\ t_1 \end{pmatrix} \tag{38}$$

where x_1, z_1, t_1 are byproducts of the choice of k_1, k_2, k_3 and u and S_1 is symplectic. ♦

Substep 2: Then, as in lemma 1, we find $v, w, k_4, k_5 \in \mathbb{Z}_d$ such that

$$\left\{\begin{array}{l} vz_1 + wt_1 = z_1 \wedge t_1 = z_2 \\ -k_5 z_1 + k_4 t_1 = 0 \\ vk_4 + wk_5 = 1 \end{array}\right. , \tag{39}$$

and we perform a second left-multiplication:

$$\underbrace{\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & v & w \\ 0 & 0 & -k_5 & k_4 \end{pmatrix}}_{S_2} \begin{pmatrix} x_1 \\ \delta \\ z_1 \\ t_1 \end{pmatrix} = \begin{pmatrix} x_1 \\ \delta \\ z_2 \\ 0 \end{pmatrix}, \tag{40}$$

where S_2 is a symplectic matrix. ♦

Substep 3: Since

$$\delta = x \wedge y \wedge z \wedge t = x_1 \wedge \delta \wedge z_1 \wedge t_1 = x_1 \wedge \delta \wedge z_2, \tag{41}$$

we also have

$$\delta \wedge z_2 = (x_1 \wedge \delta \wedge z_2) \wedge z_2 = \delta. \tag{42}$$

Thus we can find k_6 such that $k_6 \delta + z_2 = 0$ and we perform a third left-mutiplication:

$$\underbrace{\begin{pmatrix} 1 & 0 & 0 & k_6 \\ 0 & 1 & 0 & 0 \\ 0 & k_6 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}}_{S_3} \begin{pmatrix} x_1 \\ \delta \\ z_2 \\ 0 \end{pmatrix} = \begin{pmatrix} x_1 \\ \delta \\ 0 \\ 0 \end{pmatrix}, \tag{43}$$

where S_3 is symplectic. ♦

If $n > 2$, we apply the process defined by this sequence of substeps $n-1$ times in order to end with a vector whose components are null except maybe the first two ones. At step i, we set the $(2n+2-2i)$-th and the $(2n-2i+1)$-th components to 0. For a single vector, we can go further and set the second component to 0 as in the second substep above. We shall soon define a substep 4 to complete this list of elementary operations.

It is in general not possible to diagonalise nor to trigonalise a matrix using only a left-multiplication by a symplectic matrix. For instance, let us try to do even weaker a job with the matrix B in the following equality over $\mathbb{Z}/p^s\mathbb{Z}$, $s \geq 1$:

$$\underbrace{\begin{pmatrix} \alpha & * & \gamma & k_1 \\ \beta & * & \delta & k_2 \\ 0 & * & l_1 p & * \\ 0 & * & l_2 p & * \end{pmatrix}}_{L} \underbrace{\begin{pmatrix} 1 & 0 \\ 0 & p \\ 0 & 1 \\ 0 & 0 \end{pmatrix}}_{B} = \begin{pmatrix} \alpha & * \\ \beta & * \\ 0 & 0 \\ 0 & 0 \end{pmatrix}. \tag{44}$$

Our aim is to find a symplectic matrix L so as to get rid of any nonzero term in the last two rows. The first, third and fourth column vectors of L, let us call them C_1, C_3 and C_4, must be as shown in (44). But as L is supposed to be sympletic, C_3 must be free and $\omega(C_1, C_3) = 0$. So there exist $k_3, k_4 \in \mathbb{Z}_d$ such that $k_3\gamma + k_4\delta = 1$ and $\alpha\delta = \beta\gamma$. Hence (α, β) is a multiple of (γ, δ):

$$\alpha = (k_3\gamma + k_4\delta)\alpha = (k_3\alpha + k_4\beta)\gamma, \tag{45a}$$

$$\beta = (k_3\gamma + k_4\delta)\beta = (k_3\alpha + k_4\beta)\delta. \tag{45b}$$

Since C_1 has to be free, $(k_3\alpha + k_4\beta)$ has to be a unit. Then there exists $l \in \mathbb{Z}_d$ such that

$$\omega(C_1, C_4) = k_2\alpha - k_1\beta = (k_3\alpha + k_4\beta)(k_2\gamma - k_1\delta) = (k_3\alpha + k_4\beta)(\omega(C_3, C_4) - lp). \tag{46}$$

That quantity should be both 0 and invertible and L cannot be symplectic. As for simple reduction, we shall make use of right-multiplications to complete the reduction. Still, it is only possible to lower-trigonalise that way. Despite that restrictive result, we are to find another way of reducing that will prove sufficient to study Lagrangian submodules in Section 3. We shall also need the

Criterion 6 *Let $a, x, y, z \in \mathbb{Z}_d$, $a \neq 0$, x a multiple of a and*

$$m = \begin{pmatrix} a & x \\ 0 & y \\ 0 & z \\ 0 & 0 \end{pmatrix}. \tag{47}$$

There exists a symplectic matrix S such that Sm is upper-triangular iff z is multiple of y.

Proof. If z is multiple of y, we can trigonalise m by applying substep 3.

Given $a, x, y, z \in \mathbb{Z}_d$ as specified in the criterion, $\delta = y \wedge z$ on the one hand and $k \in \mathbb{Z}_d, v \in U(\mathbb{Z}_d)$ on the other hand such that $\delta = ky + vz$, we have

$$\underbrace{\begin{pmatrix} 1 & 0 & 0 & kv^{-1} \\ 0 & 1 & 0 & 0 \\ 0 & k & v & 0 \\ 0 & 0 & 0 & v^{-1} \end{pmatrix}}_{S_4} \underbrace{\begin{pmatrix} a & x \\ 0 & y \\ 0 & z \\ 0 & 0 \end{pmatrix}}_{m} = \underbrace{\begin{pmatrix} a & x \\ 0 & y \\ 0 & \delta \\ 0 & 0 \end{pmatrix}}_{m'}, \tag{48}$$

where S_4 is symplectic. There exists $k' \in \mathbb{Z}_d$ such that $y = k'\delta$ and let $\nu = \nu(\delta)$. In order not to burden the argument with unessential details, we refer to the Chinese remainder theorem to suppose that d is a power of a prime, say p^s. Let $t = v_p(a) < s$. If m' is symplectically trigonalisable as set out in the criterion, the symplectic matrix to use must be as shown in the following equation:

$$\underbrace{\begin{pmatrix} w + k_{11}p^{s-t} & * & * & * \\ k_{21}p^{s-t} & w^{-1} + k_{22}p^{s-t} & k_{23}p^{s-t} & k_{24}p^{s-t} \\ k_{31}p^{s-t} & \alpha_1 & -\alpha_1 k' + l_1\nu & \beta_1 \\ k_{41}p^{s-t} & \alpha_2 & -\alpha_2 k' + l_2\nu & \beta_2 \end{pmatrix}}_{symplectic} \underbrace{\begin{pmatrix} a & x \\ 0 & y \\ 0 & \delta \\ 0 & 0 \end{pmatrix}}_{m'} = \begin{pmatrix} wa & * \\ 0 & * \\ 0 & 0 \\ 0 & 0 \end{pmatrix}, \tag{49}$$

with $w \in U(\mathbb{Z}_d)$. We leave the checking of that form to the reader. But the symplectic inner product of the third and fourth columns of that matrix has to be 1, what proves with Bézout's theorem that k' and ν are coprime. Let $\alpha, \beta \in \mathbb{Z}_d$ be such that $\alpha k' + \beta\nu = 1$. Then $\alpha y = \alpha k'\delta = (1-\beta\nu)\delta = \delta$. $\blacksquare$

We can now state our

Substep 4: Let $x, y, z \in \mathbb{Z}_d$, $\delta = y \wedge z$ and $X = (x, y, z, 0)^T$ with respect to some symplectic basis. One can find a new symplectic basis in which X is written $(x, y, \delta, 0)^T$. The way to do so is given in (48). $\blacklozenge$

In what follows, we shall need a refined version of the algorithm $\mathscr{A}$. Recall that for any $2n \times k$ matrix m, $k \geq 1$, there exists an $k \times k$ invertible matrix $R(m)$ such that $\mathscr{A}(m) = mR(m)$. For any $2n \times k$ matrix m, $i \in \{1, \ldots, 2n\}$, $j \in \{1, \ldots, k-1\}$, and $m_{[i,j]}$ the $(i, \ldots, 2n; j, \ldots, k)$ submatrix of m, $\mathscr{A}_{i,j}$ will be the algorithm defined by

$$\mathscr{A}_{i,j}(m) = m \begin{pmatrix} I_{j-1} & 0_{j-1,k-j+1} \\ 0_{k-j+1,j-1} & R(m_{[i,j]}) \end{pmatrix}. \tag{50}$$

$\mathscr{A}_{i,j}$ does essentially the same job as $\mathscr{A}$ on columns j to k of m, but it takes into account only the last $2n - i + 1$ rows to maximise the order and combines those columns on the other lines accordingly.

We now go on with the symplectic reduction algorithm for a single Chinese factor. We suppose that $d = p^s$.

Symplectic reduction algorithm $\mathscr{S}$: Suppose we are given a basis $b = (b_1, \ldots, b_k)$ of a submodule M of $\mathbb{Z}_d^{2n}$ and B is the matrix of size $2n \times k$ whose i-th column is b_i. To reduce B in a symplectic way, the sarting point is $i = j = 1$ and $B' = B$, where i and j are some counters. Then while $i \leq 2n-3$ and $j \leq k-1$, that is to say while there remain at least four lines and two columns to deal with, do:

1. Apply $\mathscr{A}_{i,j}$ to B' and perform a first left-multiplication by a symplectic matrix in order to set to 0 all the coefficients in the j-th column sarting from the $(i+1)$-th line. We obtain a matrix $B^{(1)}$.

2. Apply $\mathscr{A}_{i+1,j+1}$ to $B^{(1)}$ and perform a second left-multiplication by a symplectic matrix to set to 0 all the coefficients in the $(j+1)$-th column sarting from the $(i+4)$-th line. Indeed, as we see with the example above (equation 44), a step further as we planned to make it in the substeps could affect the j-th column in a wrong way. We obtain a matrix $B^{(2)}$ whose $(i, \ldots, i+3; j, j+1)$ submatrix is

$$\begin{pmatrix} b^{(1)}_{i,j} & b^{(1)}_{i,j+1} \\ 0 & b^{(1)}_{i+1,j+1} \\ 0 & b^{(2)}_{i+2,j+1} \\ 0 & b^{(2)}_{i+3,j+1} \end{pmatrix}. \tag{51}$$

3. Performing substeps 2 and 4, we get a matrix $B^{(3)}$ whose $(i, \dots, i+3; j, j+1)$ submatrix is of the form

$$\begin{pmatrix} b_{i,j}^{(1)} & b_{i,j+1}^{(1)} \\ 0 & xb_{i+2,j+1}^{(3)} \\ 0 & b_{i+2,j+1}^{(3)} \\ 0 & 0 \end{pmatrix}, \tag{52}$$

   with $x \in \mathbb{Z}_d$. Notice the line index on the second line.

4. If x is a unit, apply substep 3 to get a matrix $B^{(4)}$. If x is not a unit, just take $B^{(4)} = B^{(3)}$.

5. Since every coefficient in the $(i, \dots, 2n; j+1, \dots, k)$ submatrix of $B^{(4)}$ is a multiple of $b_{i,j}^{(4)} = b_{i,j}^{(1)}$, right-multiply $B^{(4)}$ by an appropriate, invertible matrix to set to 0 the coefficients on the i-th row starting from the $(j+1)$-th column. We obtain a matrix $B^{(5)}$.

6. If x is a unit, since every coefficient in the $(i+1, \dots, 2n; j+2, \dots, k)$ submatrix of $B^{(5)}$ is a multiple of $b_{i+1,j+1}^{(5)} = b_{i+1,j+1}^{(4)}$, right-multiply $B^{(5)}$ by an appropriate, invertible matrix to set to 0 the coefficients on the $(i+1)$-th row starting from the $(j+2)$-th column. We obtain a new matrix B'. If x is not a unit, just take $B' = B^{(5)}$.

7. If x is a unit, increase i and j by 2. If not, increase i by 2 and j by 1 only. In this latter case, we need not perform step 1 at the next pass. The new $B^{(1)}$ is just the new B'.

Once this repeating process has ended, if $i = 2n-1$, we reduce the last two rows by means of a simple reduction, so as to have at most two nonzero coefficients on them. If $i < 2n-1$ and $j = k$, apply a last left-multilplication by a symplectic matrix to B' so as to reduce the last column as far as possible without modifying the others. As an example, if we started with a $2n \times 2n$ matrix B with $n = 8$, we may end up with a matrix of the form

$$\mathscr{S}(B) = \left(\begin{array}{cccccccccccccccc}
* & & & & & & & & & & & & & & & \\
 & * & & & & & & & & & & & & & & \\
\hline
 & & * & & & & & & & & & & & & & \\
 & & & * & & & & & & & & & & & & \\
\hline
 & & & & * & & & & & & & & & & & \\
 & & & & & R & * & * & * & * & * & * & * & * & * & * \\
\hline
 & & & & & * & & & & & & & & & & \\
 & & & & & & * & & & & & & & & & \\
\hline
 & & & & & & & * & & & & & & & & \\
 & & & & & & & & R & * & * & * & * & * & * & * \\
\hline
 & & & & & & & & * & & & & & & & \\
 & & & & & & & & & * & & & & & & \\
\hline
 & & & & & & & & & & * & & & & & \\
 & & & & & & & & & & & * & & & & \\
\hline
 & & & & & & & & & & & & * & & & \\
 & & & & & & & & & & & & & * & &
\end{array}\right), \tag{53}$$

where the meaning of the letter R is explained below. ♦

Horizontal lines of stars in (53) beginning with an R will be called rent lines and places marked with an R rent points. It is because of rent lines that we need actual right-multiplications in steps 5 and 6 instead of merely setting some coefficients to 0 as in simple reduction. Without those right-multiplications, we should not produce a basis matrix for the very submodule we started from. A rent line can occur only on an even row. Suppose (i, j) is a rent point in the reduced matrix. Every coefficient in the $(i, \ldots, 2n; j, \ldots, k)$ submatrix is a multiple of the coefficient underneath the rent point, at position $(i + 1, j)$. So, if this coefficient is 0, we may stop the algorithm. Last but not least about rents, it was necessary to perform the algorithm in a single Chinese factor, since a rent may occur at some position in some Chinese factor while not in another one. This reduction procedure is thus linked in an essential way to the Chinese remainder theorem.

The algorithm $\mathscr{S}$ consists in choosing basis vectors $f_1, \ldots, f_{2n}$ one after the other so as to obtain a basis matrix for M of a particular form with respect to the free basis f thus constituted. But can we avoid rents by a discerning choice of the f_i's so as to get a diagonal basis matrix for M? Is it a good strategy to choose a vector of the greatest possible order as we did? If the issue of order has actually to be addressed, is it of some use to discriminate between the vectors of a given order? We shall answer those questions in Section 4, but we are now sufficiently provided to study Lagrangian submodules.

3 Lagrangian submodules

For any submodule M of $\mathbb{Z}_d^{2n}$, we define the symplectic orthogonal of M by

$$M^\omega = \{x \in \mathbb{Z}_d^{2n}; \forall y \in M, \omega(x, y) = 0\}. \tag{54}$$

A submodule M is called

- isotropic if $M \subset M^\omega$,
- coisotropic if $M^\omega \subset M$,
- symplectic if $M \cap M^\omega = \{0\}$,
- Lagrangian if $M = M^\omega$.

Let M be a Lagrangian submodule. M is isotropic. Let us suppose that there exists an isotropic submodule N such that $M \subsetneq N$. Then $M \subsetneq N \subset N^\omega \subset M^\omega$ and hence M is not Lagrangian. Thus, a Lagrangian submodule is isotropic and maximal for inclusion restricted to isotropic submodules. Theorem 7 below will show that the converse is also true.

We are going to use symplectic reduction to find a very simple form for a minimal basis matrix of M. As we saw it, we are to suppose that $d = p^s$. Let B_0 be a basis matrix for M. The symplectic reduction $B = \mathscr{S}(B_0)$ is still a basis matrix for M. Suppose some coefficient appears on an even row, say at position $(2i, j)$, without a rent. Since M is isotropic, the symplectic product of the $(2i-1)$-th and the $(2i)$-th column vectors of $\mathscr{S}(B)$ must be zero, what can be written

$$v_p(\mathscr{S}(B)_{2i-1,j-1}) + v_p(\mathscr{S}(B)_{2i,j}) \geq s. \tag{55}$$

The maximality of M implies that this is in fact an equality. On the contrary, if there is a rent point at position $(2i, j)$ and if the coefficient of $\mathscr{S}(B)$ at position $(2i-1, j-1)$ has p-valuation t, then, by maximality of M, the vector

$$C = (0, \ldots, 0, p^{s-t}, 0, \ldots, 0)^T \tag{56}$$

with p^{s-t} at the $(2i)$-th position, is in M. We insert this column at position $2i$, that is to say between the $(2i-1)$-th and the $(2i)$-th columns of $\mathscr{S}(B)$. Since M is isotropic, every coefficient on the $(2i)$-th line is a multiple of p^{s-t} and we may set to 0 every coefficient on this line at right of the new column. We apply this trick to each rent and obtain a diagonal matrix. So there exist $k \in \{1, \ldots, n\}$ and $s_1, \ldots, s_k \in \{0, \ldots, s\}$ so that the diagonal matrix

$$D = \mathrm{diag}(p^{s_1}, p^{s-s_1}, p^{s_2}, p^{s-s_2}, \ldots, p^{s_k}, p^{s-s_k}) \tag{57}$$

is a basis matrix for M. If $k < n$, then M would not be maximal. One could add for instance the vector

$$(0, \ldots, 0, 1, 0, \ldots, 0)^T \tag{58}$$

with 1 at the $(2k+1)$-th position and get a greater isotropic submodule. So $k = n$. By construction of $\mathscr{S}(B)$, $s_i \leq s_j$ whenever $i < j$. Also note that C, as a vector of M, has to be a linear combination of the column vectors of $\mathscr{S}(B)$. Since our trick to make good a rent always yields a new basis matrix for M, the same is true for every additional column. So, whether a diagonal coefficient of D on an even row appeared while dealing with a rent or not, our using of the algorithm $\mathscr{A}$ warrants that for all $i \in \{1, \ldots, n\}$, $s_i \leq s - s_i$. Since these results do not depend on the Chinese factor we chose, we have proved the

Theorem 7 *Let M be a submodule of $\mathbb{Z}_d^{2n}$ and $d = \prod_{i \in I} p_i^{s_i}$ be the prime factor decomposition of d. Then M is Lagrangian iff the following two conditions are satisfied. There exists a unique family*

$$(d_1, \ldots, d_n) \in \left\{1, \ldots, \prod_{i \in I} p_i^{\lfloor s_i/2 \rfloor}\right\}^n \tag{59}$$

such that $d_1 | d_2 | \ldots | d_n | d$ and there exists a $2n \times 2n$ symplectic matrix S such that

$$S \times \mathrm{diag}(d_1, d/d_1, d_2, d/d_2, \ldots, d_n, d/d_n) \tag{60}$$

be a basis matrix for M.

As a remark to close this section, suppose the $(2i)$-th diagonal coefficient of D, $i \in \{1, \ldots, n-1\}$, appeared while applying the algorithm $\mathscr{S}$ to B_0, that is to say there was no rent on the $(2i)$-th line. Then $s/2 \geq s_{i+1} \geq s - s_i \geq s/2$ and so, for

$j \geq i$, $s_j = s/2$. If s is odd, there is necessarily a rent on every even row of $\mathscr{S}(B_0)$ except the last one.

4 A criterion for symplectic diagonalisation

Lagrangian submodules are quite a particular case. In this section, we first prove with an example that it is not always possible, for some submodule M, to find a symplectic basis f and a $2n \times 2n$ diagonal matrix D such that fD be a basis of M. The diagonal entries of the D need not be arranged by increasing valuations. If such a pair (f, D) exists, we shall say that M is nearly symplectic. Our aim will then be to provide an criterion to know if a given M is nearly symplectic. That will be done with the algorithm $\mathscr{D}_\omega$ that also yields the symplectic basis f if any. We shall eventually see that as Lagrangian submodules, symplectic ones form a particular kind of nearly symplectic submodules. For the sake of simplicity, we take in this section $d = p^s$.

Let $c \in \{1, \ldots, 2n\}$ and $x = (x_1, \ldots, x_c)$ a family of vectors in $\mathbb{Z}_d^{2n}$. The Gram matrix of x, $G = \mathrm{Gram}(x)$, is the $c \times c$ matrix given by

$$\forall i, j \in \{1, \ldots, c\}, g_{ij} = \omega(x_i, x_j). \tag{61}$$

With matrices, if B is the representative matrix of x with respect to the computational basis e, then $G = B^T J_n B$ and thus G is antisymmetric, but not necessarily invertible, even if x is free. Yet, if $c = 2n$ and x is a free basis of $\mathbb{Z}_d^{2n}$, then $B, G \in \mathrm{GL}(2n, \mathbb{Z}_d)$. The discriminant of x is the determinant of its Gram matrix:

$$\Delta(x) = \det(\mathrm{Gram}(x)). \tag{62}$$

Let M be a submodule of $\mathbb{Z}_d^{2n}$ and F_M the set of all free bases f of $\mathbb{Z}_d^{2n}$ such that M has a diagonal basis matrix with respect to f as in theorem 3. We take the K_i's, $i \in \{0, \ldots, s\}$, to be defined as in the proof and in the commentary of that theorem in (25) and (33)[1]. Some of those intervals may be empty. By restriction, the K_i's determine a partition K' of $\{1, \ldots, c\}$:

$$\forall i \in \{0, \ldots, s\}, K_i' = K_i \cap \{1, \ldots, c\}. \tag{63}$$

For every $(i, j) \in \{0, \ldots, s\}^2$, G_{ij} will be the $(K_i'; K_j')$ block of G. We also put $\widehat{G}_{ij}$ to be a matrix so that if G_{ij} is not the empty matrix and if $s_{ij} = v_p(G_{ij})$, then $v_p\big(\widehat{G}_{ij}\big) = 0$ and $p^{s_{ij}} \widehat{G}_{ij} = G_{ij}$. The matrix $\widehat{G}_{ij}$ thus pointed out is not unique if $s_{ij} > 0$. If G_{ij} is the empty matrix, then so is $\widehat{G}_{ij}$.

For now we take $c = 2n$ only. A simplified study upon Gram matrices enables us to give the simplest example of a non-nearly-symplectic submodule. The pattern we catch a glimpse of here about those matrices will be seen in its plain form afterwards. The reader who is interested only in the general case may skip to the next part.

[1] Be careful that n has been replaced by $2n$.

Let $f \in F_M$. For all $i \in \{1, \dots, 2n\}$, we define

$$\alpha_M(f_i) = \min(v_p(\omega(f_i, x)); x \in M), \tag{64a}$$
$$\beta(f, i) = \min(j \in \{0, \dots, s\}; \exists k \in K_j, g_{ik} \in U(\mathbb{Z}_d)). \tag{64b}$$

The graph on figure 2 illustrates the meaning of $\alpha_M(f_i)$ and $\beta(f, i)$. For any k and v, a plain bullet at position (k, v) indicates that $v_p(g_{ik}) = v$.

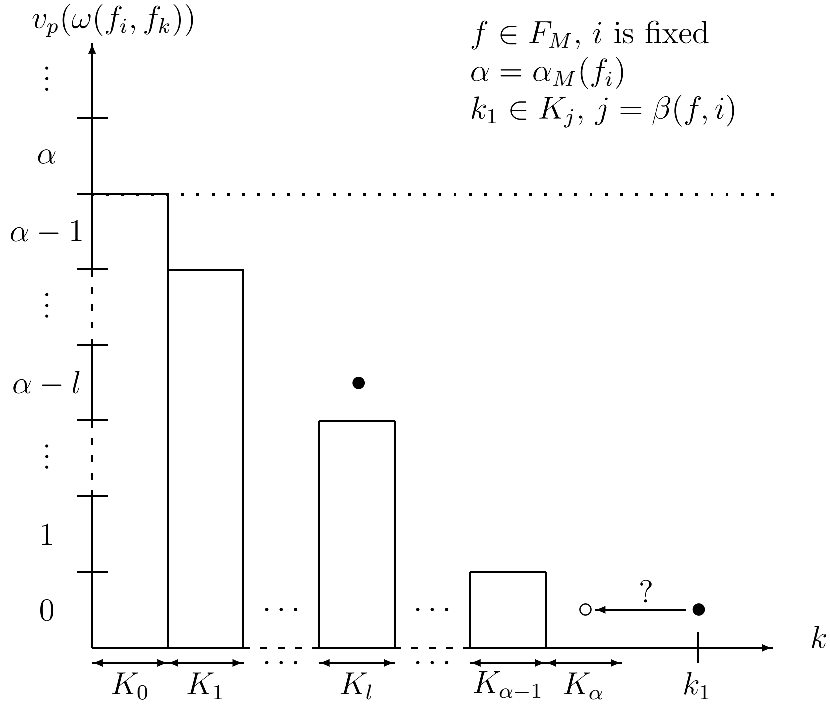

Figure 2: The functions α_M and β

So there must exist $l \in \{0, \dots, \alpha\}$ and $k_0 \in K_l$ so that $v_p(g_{ik_0}) = \alpha - l$. Let $i \in \{1, \dots, 2n\}$, $j = \beta(f, i)$ and $k_1 \in K_j$ so that $g_{ik_1} \in U(\mathbb{Z}_d)$. Then $\alpha_M(f_i) \leq v_p(\omega(f_i, p^j f_{k_1})) = j = \beta(f, i)$. This inequality is illustrated by the second plain bullet at position $(k_1, 0)$.

We then consider a nearly symplectic submodule M with a convenient pair (f, D). If $(v_p(d_{ii}))_{i=1,\dots,2n}$ is not an increasing sequence, we use a $2n \times 2n$ permutation matrix Q so that the diagonal coefficients of $Q^T D Q$ are arranged by increasing valuation. Let $f' = fQ \in F_M$. On each line of $\mathrm{Gram}(f') = Q^T J_n Q$, there is only one nonzero coefficient which is necessarily invertible, in fact 1 or -1, and it is clear that for all $i \in \{1, \dots, 2n\}$, $\alpha_M(f'_i) = \beta(f', i)$. On figure 2, the equality $\alpha_M(f_i) = \beta(f, i)$ is checked iff $k_1 \in K_\alpha$.

We are now ready to find the annouced non-nearly-symplectic submodule. Let $s > 1$ and M be the submodule generated by the column vectors of the matrix B in the following equation, with respect to e:

$$\underbrace{\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1-p & 0 \\ 0 & -1 & p & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}}_{L} \underbrace{\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & p & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}}_{B} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \tag{65}$$

We left-multiply B by an invertible matrix L so as to obtain a diagonal matrix. Here, the diagonal coefficients of that latter matrix are already arranged by increasing valuation. $K_0 = \{1, 2\}$ and $K_s = \{2, 4\}$ are the only nonempty intervals K_i. The new computational basis is $f = eL^{-1} \in F_M$ and the Gram matrix of f is

$$G = L^{-T} J_n L^{-1} = \left(\begin{array}{cc|cc} 0 & p & -1+p & 0 \\ -p & 0 & 0 & 1 \\ \hline 1-p & 0 & 0 & 1 \\ 0 & -1 & -1 & 0 \end{array}\right), \tag{66}$$

with $L^{-T} = (L^{-1})^T$. At the end of Section 1, we defined $\Sigma_{\mathscr{D}}(M)$. Here, any matrix $P \in \Sigma_{\mathscr{D}}(M)$ is of the form

$$P = \begin{pmatrix} A_1 & A_2 \\ 0_{2,2} & A_3 \end{pmatrix}, \tag{67}$$

with $A_1, A_3 \in \mathrm{GL}(2, \mathbb{Z}_d)$. The Gram matrix of $f' = fP$ is of the form

$$P^T G P = \begin{pmatrix} pA_1^T \widehat{G}_{00} A_1 & A_4 \\ -A_4 & A_5 \end{pmatrix}, \text{ with } \widehat{G}_{00} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \tag{68}$$

and $A_1^T \widehat{G}_{00} A_1, A_4 \in \mathrm{GL}(2, \mathbb{Z}_d)$. But we see that for any $i \in K_0 = \{1, 2\}$, $\alpha_M(f_i') = 1 < \beta(f', i) = s$. Comparing to the result of the previous paragraph, this proves our claim that M is not nearly symplectic.

What if $s = 1$? In that case, the matrix obtained by swapping the second and third columns of B, namely $\mathrm{diag}(1, 0, 1, 0)$, is a convenient diagonal basis matrix for M with respect to the symplectic basis e.

In the remaining part of this section, we tell how to know whether a given submodule M is nearly symplectic or not and how to find a convenient pair (f, D). We shall need a little more vocabulary. Let b be a free basis of $\mathbb{Z}_d^{2n}$, $\sigma \in \mathfrak{S}_{2n}$ a permutation of $\{1, \ldots, 2n\}$ and Q the representative matrix of σ, that is to say the only nonzero coefficients of Q are equal to 1 and are located at the positions $(i, \sigma(i))_{i=1,\ldots,2n}$. We denote b_σ the free basis $(b_{\sigma(1)}, \ldots, b_{\sigma(2n)})$ of $\mathbb{Z}_d^{2n}$ and say that b is σ-symplectic if $b_\sigma = bQ^T$ is symplectic. In that case, the representative matrix of ω in basis b is $Q^T J_n Q$. A $2n \times 2n$ matrix L is said σ-symplectic if QLQ^T is symplectic or equivalently if

$$L^T (Q^T J_n Q) L = Q^T J_n Q. \tag{69}$$

Thus the conjugation by L preserves the matrix representative of ω in b, L is invertible and L^{-1} is still σ-symplectic. If b and L are σ-symplectic, $bL = bQ^T QL$ is still a

σ-symplectic basis and if B is the representative matrix of b with respect to a σ-symplectic basis f, then B is a σ-symplectic matrix. Indeed, fQ^T and $bQ^T = (fQ^T)(QBQ^T)$ are symplectic bases and hence QBQ^T is a symplectic matrix.

The notions of scalar and set fringe we are going to define involve the K_i's and thus are meanigless unless a reference submodule or a suitable partition of $\{1,\ldots,2n\}$ is specified. Let M be a submodule of $\mathbb{Z}_d^{2n}$. Define the K_i's accordingly and let κ be the map

$$\begin{array}{rcll}\kappa: \ \{1,\ldots,2n\} & \longrightarrow & \{0,\ldots,s\}, & \text{such that } i \in K_{\kappa(i)}. \\ i & \longmapsto & \kappa(i) & \end{array} \tag{70}$$

Then for any Gram matrix G of size $\leq 2n$ and containing at least one unit, we define the scalar (M-)fringe of G by

$$\mathrm{fr}_M(G) = \min(\kappa(i)+\kappa(j); g_{ij} \in U(\mathbb{Z}_d)) \tag{71}$$

or equivalently

$$\mathrm{fr}_M(G) = \min(i+j; v_p(G_{ij}) = 0). \tag{72}$$

The (M-)fringe of G is the set of all coefficients g_{ij} such that $\kappa(i)+\kappa(j) \leq \mathrm{fr}_M(G)$. A block G_{ij} is said to be in the fringe of G if $\gamma_{ij} = \mathrm{fr}_M(G) - i - j \geq 0$. Whenever all the blocks G_{ij} in the fringe of G verify $v_p(G_{ij}) \geq \gamma_{ij}$, we shall say that the (M-)fringe of G is good. If there exists $(i,j) \in \{1,\ldots,2n\}^2$ such that

$$g_{ij} \in U(\mathbb{Z}_d) \text{ with } \gamma_{\kappa(i)\kappa(j)} = 0, \tag{73}$$

and

$$\forall k \leq i,\ v_p(g_{kj}) \geq \gamma_{\kappa(k)\kappa(j)}, \tag{74a}$$

$$\forall l \leq j,\ v_p(g_{il}) \geq \gamma_{\kappa(i)\kappa(l)}, \tag{74b}$$

we shall say that the (M-)fringe of G is nice. Of course a good M-fringe is a nice M-fringe. Let us give an example. If a block G_{ij} with $i+j=3$ contains a unit, then the following Gram matrix has a good fringe and scalar fringe 3.

$$G = \left(\begin{array}{ccccc} \boxed{p^3\widehat{G}_{00}} & \boxed{p^2\widehat{G}_{01}} & \boxed{p\widehat{G}_{02}} & \boxed{G_{03}} & \cdots \\ \boxed{p^2\widehat{G}_{10}} & \boxed{p\widehat{G}_{11}} & \boxed{G_{12}} & & \\ \boxed{p\widehat{G}_{20}} & \boxed{G_{21}} & & & \\ \boxed{G_{30}} & & & & \\ \vdots & & & & \end{array}\right). \tag{75}$$

We shall need the following lemma and corollary.

Lemma 8 *Let M be a submodule in $\mathbb{Z}_d^{2n}$. Let b be a free basis of $\mathbb{Z}_d^{2n}$ with Gram matrix G and assume that G has a good M-fringe. Then for any $P \in \Sigma_{\mathscr{D}}(M)$, P^TGP has a good M-fringe with the same scalar M-fringe as G.*

That is to say the form (75), with the particular scalar M-fringe required, is

preserved under conjugation by a matrix in $\Sigma_{\mathscr{D}}(M)$.
Proof. The reference submodule is M. Let $H = GP$. For every block H_{ij} of H, we have

$$H_{ij} = \sum_{k=0}^{j-1} G_{ik}P_{kj} + G_{ij}P_{jj} + \sum_{k=j+1}^{s} G_{ik}P_{kj}. \tag{76}$$

As to the first sum, for every $k \in \{0, \ldots, j-1\}$, we have

$$v_p(G_{ik}) + v_p(P_{kj}) \geq v_p(G_{ik}) \geq \gamma_{ik} \geq \gamma_{ij} + 1 \tag{77}$$

and we refer to relations (127a) and (127b) of Appendix A.2 to see that

$$v_p(G_{ik}P_{kj}) \geq \min(v_p(G_{ik}) + v_p(P_{kj}), s) \geq \gamma_{ij} + 1. \tag{78}$$

Since P_{jj} is invertible, the lines of $G_{ij}P_{jj}$ are of the same order as the lines of G_{ij} respectively and then

$$v_p(G_{ij}P_{jj}) = v_p(G_{ij}) \geq \gamma_{ij}. \tag{79}$$

As to the second sum, for every $k \in \{j+1, \ldots, s\}$, the inequality

$$v_p(G_{ik}) + v_p(P_{kj}) \geq (\mathrm{fr}(G) - i - k) + (k - j) = \gamma_{ij} \tag{80}$$

implies that

$$v_p(G_{ik}P_{kj}) \geq \gamma_{ij}. \tag{81}$$

So $v_p(H_{ij}) \geq \gamma_{ij}$. Let (i, j) be such that $\gamma_{ij} = 0$ and $v_p(G_{ij}) = 0$. Then the inequality in (80) may be modified as

$$\forall k \in \{j+1, \ldots, s\}, v_p(G_{ik}) + v_p(P_{kj}) \geq 0 + (k - j) \geq 1, \tag{82}$$

and we see that $v_p(H_{ij}) = 0$. So H has a good fringe with scalar fringe $\mathrm{fr}(G)$. In the same manner, $P^T GP = P^T H$ has a good fringe with scalar fringe $\mathrm{fr}(G)$. ■

Corollary 9 *Let M be a nearly symplectic submodule of $\mathbb{Z}_d^{2n}$ and $f \in F_M$. Then the matrix* $\mathrm{Gram}(f)$ *has a good M-fringe.*

Proof. By assumption, there exists $\sigma \in \mathfrak{S}_{2n}$ and f' a σ-symplectic basis in F_M. We have already seen that $G' = \mathrm{Gram}(f')$ has a good fringe (with respect to any submodule). Besides, there exists $P \in \Sigma_{\mathscr{D}}(M)$ so that $f = f'P$. So, $\mathrm{Gram}(f) = P^T G' P$ has a good M-fringe. ■

We can now give the algorithm for symplectic diagonalisation whenever possible:

Algorithm $\mathscr{D}_\omega$: Let M be a submodule of $\mathbb{Z}_d^{2n}$, b a basis of M and B its representative basis matrix with respect to any computational basis e'.

Let $f = e'L(B)^{-1} \in F_M$, where $L(B)$ was defined within the algorithm $\mathscr{D}_0$ (see page 7), $\widetilde{M} = M$ and b' be the empty sequence with values in $\mathbb{Z}_d^{2n}$. Let also c be a counter with initial value 0.

While $G = \mathrm{Gram}(f)$ has a nice $\widetilde{M}$-fringe, do

1. Choose a pair $(i,j) \in \{1,\ldots,2n-2c\}^2$ that verifies conditions (73) and (74) and perform the partial Gram-Schmidt orthogonalisation process:

$$f'_i = f_i, \quad f'_j = f_j, \tag{83a}$$

$$\forall k \in \{1,\ldots,2n-2c\} \setminus \{i,j\}, f'_k = f_k - g_{ij}^{-1} g_{ik} f_j + g_{ij}^{-1} g_{jk} f_i. \tag{83b}$$

   Owing to the nice fringe condition, the corresponding change of basis matrix R is in $\Sigma_{\mathscr{D}}(M)$. With $i \leq j$ and $g_{ij} = 1$, it reads

$$R = \left(\begin{array}{ccccccccccc}
1 & & & & & & & & & & \\
 & \ddots & & & & & & & & & \\
 & & 1 & & & & & & & & \\
\hline
g_{j1} & \cdots & g_{j,i-1} & 1 & g_{j,i+1} & \cdots & g_{j,j-1} & 0 & g_{j,j+1} & \cdots & g_{j,2n} \\
\hline
 & & & & 1 & & & & & & \\
 & & & & & \ddots & & & & & \\
 & & & & & & 1 & & & & \\
\hline
-g_{i1} & \cdots & -g_{i,i-1} & 0 & -g_{i,i+1} & \cdots & -g_{i,j-1} & 1 & -g_{i,j+1} & \cdots & -g_{i,2n} \\
\hline
 & & & & & & & & 1 & & \\
 & & & & & & & & & \ddots & \\
 & & & & & & & & & & 1
\end{array}\right), \tag{84}$$

   where the two special rows are the i-th one and the j-th one respectively. For any $k \in \{1,\ldots,2n-2c\} \setminus \{i,j\}$, $f'_k \in \langle f'_i, f'_j \rangle^{\omega}$ and since $R \in \Sigma_{\mathscr{D}}(M)$, $f' = fR \in F_M$.

2. Let b' be the concatenation of b' and $(g_{ij}^{-1} f'_i, f'_j)$.

3. Rename $\widetilde{M} \cap \langle f'_i, f'_j \rangle^{\omega}$ as $\widetilde{M}$.

4. Rename $f' \setminus \{f'_i, f'_j\}$ as f.

5. Increase c by 1.

Whenever $\mathscr{D}_\omega(b) = \mathscr{D}_\omega(e', B) = b'$ has cardinality $2n$, then it is a symplectic basis of $\mathbb{Z}_d^{2n}$, M is nearly symplectic and there exists $\sigma \in \mathfrak{S}_{2n}$ so that $b'_\sigma \in F_M$. ♦

Since $e' L(B)^{-1}$ is a free basis of $\mathbb{Z}_d^{2n}$, its Gram matrix is invertible and thus has a well-defined M-fringe. Then the discriminant

$$\Delta(f' \setminus \{f'_i, f'_j\}) = \pm \Delta(f') = \pm \det(R)^2 \Delta(f) \tag{85}$$

being a unit, all the forthcoming matrices G have a well-defined $\widetilde{M}$-fringe and $\mathscr{D}_\omega$ is a valid algorithm. Now if M is nearly symplectic, does this algorithm yields the matrix b' we search for? Besides, in step 1, the pair (i,j) is not unique. So we are to prove that if M is nearly symplectic, the algorithm $\mathscr{D}_\omega$, with any choice of the pairs, builds a symplectic basis b' that endows M with a diagonal basis matrix.

Let M be a nearly symplectic submodule of $\mathbb{Z}_d^{2n}$, $\sigma \in \mathfrak{S}_{2n}$ with representative matrix Q and h a σ-symplectic basis in F_M. Let also B be a basis matrix of M with respect to any computational basis e' and let us carry out the algorithm. Corollary 9 shows that the first Gram matrix G has a nice M-fringe. We choose a convenient pair (i, j) and find the first two vectors of b' by performing steps 1 and 2. Then with $N = M \cap \langle f'_i, f'_j \rangle^\omega$, we want to show that the Gram matrix of $f^\flat = f' \setminus \{f'_i, f'_j\}$ has a nice N-fringe. From now on, we consider N as a submodule of $\langle f^\flat \rangle$ exclusively. With that convention, $f^\flat \in F_N$ and corollary 9 tells us that it suffices to show that N is nearly symplectic.

There exists $P \in \Sigma_{\mathscr{D}}(M)$ such that $f' = hP$. For any $m \in \{1, \ldots, 2n\}$, let $\ell(m)$ be the index defined by $\omega(h_m, h_{\ell(m)}) = \pm 1$. Since $\mathrm{fr}_M(h) = \mathrm{fr}_M(f')$ as shown by lemma 8, we have

$$\kappa(m) + \kappa(\ell(m)) \geq \kappa(i) + \kappa(j) \tag{86}$$

and hence

$$\kappa(m) < \kappa(i) \Rightarrow \kappa(\ell(m)) > \kappa(j), \tag{87a}$$

$$\kappa(m) < \kappa(j) \Rightarrow \kappa(\ell(m)) > \kappa(i). \tag{87b}$$

So, and because $\omega(f'_i, f'_j) = g_{ij}$ is a unit, there exist $k \in K_{\kappa(i)}$ and $l = \ell(k) \in K_{\kappa(j)}$ so that the coefficients p_{ki} and p_{lj} in P are units. So QP has a unit on its $\sigma^{-1}(k)$-th line. Let L be a symplectic matrix so that LQP has all but its $\sigma^{-1}(k)$-th coefficient equal to 0. Since we suppose we know where an invertible coefficient is in the i-th column of P, the substeps of the symplectic reduction algorithm are unuseful to find L. Instead, we form a symplectic matrix inspired by the Gaussian reduction. For instance, if $\sigma^{-1}(k) = 1$, then $\sigma^{-1}(l) = 2$ and L is of the form

$$L = \begin{pmatrix} 1 & & & & & & \\ k_0 & 1 & -k_4 & k_3 & \cdots & -k_{2n} & k_{2n-1} \\ k_3 & & 1 & & & & \\ k_4 & & & 1 & & & \\ \vdots & & & & \ddots & & \\ k_{2n-1} & & & & & 1 & \\ k_{2n} & & & & & & 1 \end{pmatrix}. \tag{88}$$

Then the i-th column of $P' = Q^T LQP$ has all but its k-th coefficient equal to 0. The basis $h' = hQ^T L^{-1} Q$ is still σ-symplectic and $f' = hP = h'P'$. Moreover, the matrix $Z = Q^T LQ$ is in $\Sigma_{\mathscr{D}}(M)$ and thus $P' \in \Sigma_{\mathscr{D}}(M)$. Indeed, the coefficients in the k-th column of Z have the right valuations by construction. The coefficients on the l-th row not in the k-th nor in the l-th columns were determined so that Z is σ-symplectic. In particular:

$$\forall m \in \{1, \ldots, l-1\} \setminus \{k\}, \omega(Z_m, Z_k) = \pm z_{\ell(m),k} \pm z_{lm} = 0, \tag{89}$$

where for all i, Z_i is the i-th column vector of Z. And according to relation (86),

$$\forall m \in \{1, \ldots, l-1\} \setminus \{k\}, v_p(z_{\ell(m),k}) \geq \kappa(\ell(m)) - \kappa(i) \geq \kappa(l) - \kappa(m). \tag{90}$$

Thus $v_p(z_{lm}) \geq \kappa(l) - \kappa(m)$ and that proves that $Z \in \Sigma_{\mathscr{D}}(M)$. The coefficient p'_{lj} divides g_{ij} and hence is a unit. So we apply the same kind of reduction as before to the j-th column of P' while preserving the i-th one and find a σ-symplectic basis h'' and an invertible matrix $P'' \in \Sigma_{\mathscr{D}}(M)$ so that $f' = h''P''$. We may suppose without loss of generality that $g_{ij} = 1$. Then the vectors h''_k and h''_l may be redefined under a multiplication by a unit factor so that $p''_{ki} = p''_{lj} = 1$. If we assume that $i < j$ and $k < l$ for instance, P'' is of the form

$$P'' = \begin{array}{cl} \left(\begin{array}{c|c|c|c|c} * & & * & & * \\ \hline & 1 & & 0 & \\ \hline * & & * & & * \\ \hline & 0 & & 1 & \\ \hline * & & * & & * \end{array}\right) & \begin{array}{l} \\ \leftarrow \quad k \\ \\ \leftarrow \quad l \\ \\ \end{array} \\ \begin{array}{ccccc} & \uparrow & & \uparrow & \\ & i & & j & \end{array} & \end{array} \tag{91}$$

Let $h^\flat = h'' \setminus \{h''_i, h''_j\}$ and $P^\flat$ be the matrix obtained by deleting the k-th and l-th rows as well as the i-th and j-th columns of P''. Now $f'_i = h''_k$ and $f'_j = h''_l$ so that $f^\flat = h^\flat P^\flat$. By construction, $P^\flat \in \Sigma_{\mathscr{D}}(N)$. So $h^\flat \in F_N$. But since h'' is σ-symplectic and $\omega(h''_k, h''_l) = 1$, there exists $\rho \in \mathfrak{S}_{2n-2}$ such that $h^\flat$ is ρ-symplectic. That proves that N is nearly symplectic.

We end this section with a proposition that shows the difference between symplectic and nearly symplectic submodules.

Proposition 10 *Let M be a submodule of $\mathbb{Z}_d^{2n}$. Then M is symplectic iff M is nearly symplectic and such that $M + M^\omega = \mathbb{Z}_d^{2n}$. In that case, M is free and of even rank.*

Proof. If $M = \{0\}$, both terms of the equivalence are checked and M is obviously free and of even rank. So let M be a nonzero symplectic submodule and let $f \in F_M$. Since $p^{s-1} f_1 \in M \setminus \{0\}$ and $M \cap M^\omega = \{0\}$, there exists $x = \sum_{i=2}^{2n} x_i f_i \in M$ such that $\omega(p^{s-1} f_1, x) \neq 0$. Thus x is free, $\omega(f_1, x)$ is a unit, there exists $j \in K_0 \setminus \{1\}$ so that $\omega(f_1, f_j)$ is a unit and $f_1 \in M$. That proves that $\mathrm{Gram}(f)$ has a good fringe. We then perform the partial Gram-Schmidt process and find a new basis $f' \in F_M$:

$$f'_1 = f_1, \quad f'_j = f_j, \tag{92a}$$

$$\forall k \in \{1, \ldots, 2n\} \setminus \{1, j\}, f'_k = f_k - g_{1j}^{-1} g_{1k} f_j + g_{1j}^{-1} g_{jk} f_1. \tag{92b}$$

Since $2, j \in K_0$, we may rename without loss of generality f'_j as f'_2 and f'_2 as f'_j. Let $N = M \cap \langle f'_1, f'_2 \rangle^\omega$ and let y be some nonzero vector in N if any:

$$y = \sum_{i=3}^{r} y_i f'_i \in N \setminus \{0\}, \tag{93}$$

with r the rank of M. Since M is symplectic, there exists $z \in M$ so that $\omega(y, z) \neq 0$:

$$z = \sum_{i=1}^{r} z_i f_i' \in M. \tag{94}$$

But with $z' = z - z_1 f_1' - z_2 f_2' \in N$, we also have $\omega(y, z') = \omega(y, z) \neq 0$. Hence $y \notin N^\omega$ and N is symplectic. If M is larger than $\langle f_1', f_2' \rangle$, then $N \neq \emptyset$. We carry out again the same reasoning until we find a free basis h of $\mathbb{Z}_d^{2n}$ the first r vectors of which form a symplectic basis of M. Moreover, the last $2n - r$ vectors of h form a free basis $h^\flat$ of M^ω. Up to now, we proved that M is free, of even rank and such that $M \oplus M^\omega = \mathbb{Z}_d^{2n}$.

Since $\Delta(h^\flat) = \Delta(h)$ is a unit, then in the same manner as we showed the validity of $\mathscr{D}_\omega$, we see that we can apply the entire Gram-Schmidt orthogonalisation process to $h^\flat$. Hence, M is nearly symplectic.

Let us show the converse. Let f be a symplectic basis of $\mathbb{Z}_d^{2n}$ and D the following $2n \times 2n$ diagonal matrix such that fD is a basis matrix for M:

$$D = \operatorname{diag}(p^{s_1}, p^{s_2}, \ldots, p^{s_{2n-1}}, p^{s_{2n}}). \tag{95}$$

Then this other diagonal matrix D' is such that fD' is a basis matrix for M^ω:

$$D' = \operatorname{diag}(p^{s-s_2}, p^{s-s_1}, \ldots, p^{s-s_{2n}}, p^{s-s_{2n-1}}). \tag{96}$$

Under the assumption that $M + M^\omega = \mathbb{Z}_d^{2n}$, we have

$$s_1 < s \Rightarrow s - s_1 \geq 1 \Rightarrow s_2 = 0 \Rightarrow s - s_2 \geq 1 \Rightarrow s_1 = 0. \tag{97}$$

The same reasoning is true starting with any $i \neq 1$ and thus M is free: Each of the d_{ii}'s is either 1 or 0. For any $i \in \{1, \ldots, n\}$, suppose that $f_{2i} \in M$ and let $x \in M, y \in M^\omega$ so that $f_{2i-1} = x + y$. Then

$$\omega(x, f_{2i}) = \omega(x + y, f_{2i}) = 1. \tag{98}$$

That proves that the component of x along f_{2i-1} is 1 and hence $f_{2i-1} \in M$. By the same token, f_{2i} is in M if f_{2i-1} is. Therefore M is symplectic and of even rank. ∎

Conclusion

In the present work, we addressed fundamental issues about submodules over $\mathbb{Z}_d$ motivated by the growing interest for quantum information. We saw several kinds of reduction methods for a basis matrix of a finitely generated submodule over $\mathbb{Z}_d$. As a first result, we established two algorithms in order to perform simple and symplectic reduction, namely $\mathscr{D}$ and $\mathscr{S}$ respectively. In simple reduction, no conditions are imposed on the computational bases, so that one is able to get a diagonal basis matrix of the particular form specified in theorem 3 for any submodule. In symplectic reduction, only symplectic computational bases are allowed. The algorithm $\mathscr{S}$ fails to provide a diagonal basis matrix in the general case as it meets with the rent problem. But as a second result, this algorithm was enough for us to obtain an explicit description of Lagrangian submodules with respect to symplectic computational bases, as we stated in theorem 7. Outside its native area of study, such a description can be of particular interest in the construction of Wigner functions over a discrete phase space and of the corresponding marginal probabilities.

As a third result, we showed that there exist submodules with no diagonal basis matrix with respect to any symplectic computational basis. We called the submodules that have such a basis matrix nearly symplectic and gave an algorithm, namely $\mathscr{D}_\omega$, to find a suitable symplectic basis and the corresponding diagonal basis matrix. We also compared nearly symplectic submodules with symplectic ones: A symplectic submodule is nearly symplectic but its sum with its orthogonal generates $\mathbb{Z}_d^{2n}$ as a whole. Since the core feature in the area of quantum information we started from is the symplectic inner product, it is of particular interest to express the relevant submodules in as simple a way as possible whereas the way to compute a symplectic product is preserved. Thus, we would also like to know if the tools involved in the algorithm $\mathscr{D}_\omega$ enable us to perform simultaneous reduction of matrices for instance. Do all these patterns enable us to measure a kind of distance between the submodules?

Let us say more about the idea behind the symplectic product. The fundamental operation to compute such a product consists in mixing the components of the two vectors involved following a "cross" pattern. That basic pattern is found again in the wedge product and in its generalised form in the computation of determinants. In a forthcoming paper, we shall address the issue of finite projective nets over $\mathbb{Z}_d$, where the wedge product plays a particular role in relation with other geometrical objects pointed out by quantum information theory, as for example MUBs. Moreover, one commonly refers to a 2×2 determinant to know whether two qubits are entangled or not. Thus we are also to see that determinants and sums of them are a kind of measure for entanglement.

Acknowledgments

The author has carried out this work in the frame of his PhD Thesis. He wishes to thank Michel Planat and Metod Saniga for interesting discussions about discrete geometry for quantum information and his advisor Maurice Kibler for useful remarks and suggestions.

Appendix A Arithmetics in $\mathbb{Z}$ and $\mathbb{Z}_d$

A.1 gcd, lcm and order

In $\mathbb{Z}$, the notion of greatest common divisor (gcd for short) has an intuitive meaning. But it is equivalent to a little bit more abstract property which will generalise to residue class rings $\mathbb{Z}_d = \mathbb{Z}/d\mathbb{Z}$, $d \geq 2$. This equivalence is called Bézout's theorem. To see how it works, note that the sets of the form $k\mathbb{Z}$, $k \in \mathbb{Z}$, are the sole subrings of $\mathbb{Z}$. Bézout's theorem states that if δ is the gcd of $a_1, \ldots, a_n \in \mathbb{Z}$:

$$\delta = \bigwedge_{i=1}^{n} a_i, \tag{99}$$

then δ is characterised up to its sign by the set equation

$$\delta\mathbb{Z} = \sum_{i=1}^{n} a_i \mathbb{Z}, \tag{100}$$

that is to say $\delta\mathbb{Z}$ is the set of all linear combinations of the a_i's over $\mathbb{Z}$. We immediately deduce from that theorem Gauss's theorem for integers: If a divides the product bc and is coprime with b then a divides c. It is also quite obvious from Bézout's theorem that the following three properties are equivalent:

1. a is coprime with d;
2. The residue class $\overline{a}$ in the quotient ring $\mathbb{Z}_d$ is invertible. In that case, we also say that a is invertible modulo d;
3. $\overline{a}$ is a generator of $\mathbb{Z}_d$:

$$\overline{a}\mathbb{Z}_d = \{\overline{a}x; x \in \mathbb{Z}_d\} = \mathbb{Z}_d. \tag{101}$$

The invertible elements of $\mathbb{Z}_d$ are also called its units and hence their set is denoted $U(\mathbb{Z}_d)$, or $\mathbb{Z}_d^*$.

In the case of $\mathbb{Z}_d$, equation (100) is retained in order to define a notion of gcd. A residue $\overline{\delta} \in \mathbb{Z}_d$ is a gcd for a set of $\overline{a_i}$'s in $\mathbb{Z}_d$ if

$$\overline{\delta}\mathbb{Z}_d = \sum_{i=1}^{n} \overline{a_i}\mathbb{Z}_d. \tag{102}$$

So, if δ is the gcd of the a_i's, $\overline{\delta}$ is a gcd for the $\overline{a_i}$'s. As for $\mathbb{Z}$, this gcd is determined only up to an invertible mutiplier. We shall prove that later on in Section A.2. The computation of a gcd is still associative and commutative. As is the case for $\mathbb{Z}$, the $\overline{a_i}$'s will be said coprime if $\overline{\delta}$ is invertible. In this case, $\overline{\delta}\mathbb{Z}_d = \mathbb{Z}_d$. The interpretation in terms of linear combinations is still valid. The intuive one in terms of prime factor decomposition or division order is also still valid if one takes into account the slight modification indicated by the following property:

$$\overline{\delta} = \bigwedge_{i=1}^{n} \overline{a_i} \text{ in } \mathbb{Z}_d \text{ iff } \delta \wedge d = \left(\bigwedge_{i=1}^{n} a_i\right) \wedge d \text{ in } \mathbb{Z}. \tag{103}$$

Indeed, if we come back to representatives of residue classes, definition (102) reads

$$\delta\mathbb{Z} + d\mathbb{Z} = \left(\sum_{i=1}^{n} a_i\mathbb{Z}\right) + d\mathbb{Z}, \tag{104}$$

which is nothing but the second member of equivalence (103). So, there is an additional d in each member of that latter expression. It means that the power k of a prime factor in δ or in any one of the a_i's must first be replaced by the minimum of k and the power of the same prime factor in d. Light will be shed on that recipe in Section A.2 with the Chinese remainder theorem and p-adic decomposition.

If $\overline{\delta}$ is a gcd for the $\overline{a_i}$'s, we shall call $\overline{\delta \wedge d}$ *the* gcd of the $\overline{a_i}$'s. In fact, it is a gcd and if $\overline{\delta_1}$ and $\overline{\delta_2}$ are two gcd's then according to (103)

$$\overline{\delta_1 \wedge d} = \overline{\delta_2 \wedge d}. \tag{105}$$

That gcd is also the first one according to the lexicographic order from $\overline{0}$ to $\overline{d-1}$ since for any positive δ such that $\overline{\delta}$ is a gcd, $\delta \wedge d \leq \delta$.

In the same manner, we define a lowest common multiple (lcm for short) in of $a_1, \ldots, a_n \in \mathbb{Z}$ (resp. in $\overline{a_1}, \ldots, \overline{a_n} \in \mathbb{Z}_d$) to be an element μ_1 (resp. $\overline{\mu_2}$) such that

$$\mu_1 \mathbb{Z} = \bigcap_{i=1}^{n} a_i \mathbb{Z} \qquad \left(\text{resp. } \overline{\mu_2}\mathbb{Z}_d = \bigcap_{i=1}^{n} \overline{a_i}\mathbb{Z}_d\right). \tag{106}$$

The lcm operation is associative and commutative in both case and is denoted by the vee symbol $\vee$:

$$\mu_1 = \bigvee_{i=1}^{n} a_i \qquad \left(\text{resp. } \overline{\mu_2} = \bigvee_{i=1}^{n} \overline{a_i}\right). \tag{107}$$

Those two notions of lcm's are related by

$$\overline{\mu} = \bigvee_{i=1}^{n} \overline{a_i} \text{ in } \mathbb{Z}_d \text{ iff } \mu \wedge d = \left(\bigvee_{i=1}^{n} a_i\right) \wedge d \text{ in } \mathbb{Z}. \tag{108}$$

Indeed, since the map $x \mapsto \overline{x}$ is onto, the first equality means

$$\mu\mathbb{Z} + d\mathbb{Z} = \bigcap_{i=1}^{n}(a_i\mathbb{Z} + d\mathbb{Z}) \tag{109}$$

and the second one means

$$\mu\mathbb{Z} + d\mathbb{Z} = \left(\bigcap_{i=1}^{n} a_i\mathbb{Z}\right) + d\mathbb{Z}. \tag{110}$$

We are thus to prove that

$$\bigcap_{i=1}^{n}(a_i\mathbb{Z} + d\mathbb{Z}) = \left(\bigcap_{i=1}^{n} a_i\mathbb{Z}\right) + d\mathbb{Z}. \tag{111}$$

Since all operations involved here are associative and the intersection of two subrings is still a subring, we can prove this equality by induction. So let us suppose that

$n = 2$ and let x be in the first set:

$$x = k_1 a_1 + l_1 d = k_2 a_2 + l_2 d. \tag{112}$$

Divide each member by $a_1 \wedge a_2 \wedge d$:

$$x' = k_1 a_1' + l_1 d' = k_2 a_2' + l_2 d'. \tag{113}$$

Then $a_1' \wedge a_2'$ divides $k_1 a_1' - k_2 a_2' = (l_2 - l_1)d'$ and is coprime with d'. So there exist $n_1, n_2 \in \mathbb{Z}$ so that $n_1 a_1' - n_2 a_2' = l_2 - l_1$. Let us call $y = n_1 a_1' + l_1 = n_2 a_2' + l_2$. We have

$$x' - yd' = (k_1 - n_1 d')a_1' = (k_2 - n_2 d')a_2' \tag{114}$$

and eventually

$$x - yd \in \bigcap_{i=1}^{n} a_i \mathbb{Z}. \tag{115}$$

The converse inclusion for (111) is trivial. Note that (111) was quite obvious with the prime factor decomposition interpretation of gcd and lcm since each of those two operations in $\mathbb{Z}$ is distributive with respect to the other.

Finally, we define the order $\nu(a)$ of $a \in \mathbb{Z}_d$ to be the cardinality of the subring $a\mathbb{Z}_d = \{ka; k \in \mathbb{Z}_d\}$. This is also the first positive natural number n such that na is a multiple of d. The only residue whose order is 1 is 0, a is invertible modulo d iff $\nu(a) = d$, and $\nu(a)\mathbb{Z}$ is the kernel of the linear map

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z}_d \\ k & \longmapsto & ka. \end{array} \tag{116}$$

We know from group theory that the cardinality of a subgroup H of a finite group G is a divisor of the cardinality of G. For any $a \in \mathbb{Z}$, since $\overline{a}\mathbb{Z}_d$ is a subgroup of $\mathbb{Z}_d$, $x = d/\nu(\overline{a})$ is a well-defined integer such that the order of $\overline{x}$ is $\nu(\overline{a})$. Let us carry out the Euclidean division of a by x: $a = qx + r$ with $0 \leq r < x$ and suppose that $r \neq 0$. From the definition of r and according to that latter assumption, $\nu(\overline{r}) > \nu(\overline{x}) = \nu(\overline{a})$. But $\nu(\overline{a})\overline{r} = \nu(\overline{a})\overline{a} - \overline{q}(\nu(\overline{a})\overline{x}) = 0$ so that $\nu(\overline{r}) \leq \nu(\overline{a})$, contradiction. Thus $\overline{a} \in \overline{x}\mathbb{Z}_d$ and $\overline{a}\mathbb{Z}_d \subset \overline{x}\mathbb{Z}_d$. Since those two sets have the same cardinality they are equal and we have just seen that no residue class $\overline{r}$ with $0 \leq r < x$ can generate this set, except for the case when $\overline{a} = \overline{x} = \overline{r} = 0$. We deduce that $\overline{x}$ is the gcd of the one-element family $(\overline{a})$. We shall say that it is the gcd of the element $\overline{a}$.

So, we can compute the order of $\overline{a}$ as

$$\nu(\overline{a}) = \frac{d}{a \wedge d}. \tag{117}$$

It means that if

$$d = \prod_{i=1}^{n} p_i^{s_i} \text{ and } a = \prod_{i=1}^{n} p_i^{s_i'} \prod_{j=1}^{m} p_j^{s_j''} \tag{118}$$

are the prime factor decompositions of d and a, then

$$\nu(\overline{a}) = \prod_{i=1}^{n} p_i^{s_i - \min(s_i, s_i')}. \tag{119}$$

Hence we can find again the equivalence we first deduced from Bézout's theorem.

A.2 The Chinese remainder theorem

In the previous section of this appendix, we saw that $\overline{a}\mathbb{Z}_d = \overline{x}\mathbb{Z}_d$ with $x = a \wedge d$. We may wonder from $\nu(\overline{a}) = \nu(\overline{x})$ and from (118) and (119) if there is no invertible factor $\lambda \in \mathbb{Z}_d$ such that $\overline{a} = \lambda\overline{x}$. Moreover, it will prove the claim after (102) that the gcd is determined up to an invertible factor. Since if δ_1 and δ_2 are two possible gcd's, then there shall exist two invertible λ_1 and λ_2 such that

$$\delta_k = \lambda_k \overline{\left(\frac{d}{\nu(\delta_k)}\right)} \text{ for } k = 1, 2, \tag{120}$$

and so $\delta_2 = \lambda_2\lambda_1^{-1}\delta_1$. It will also proves that for any gcd δ of the $\overline{a_i}$'s, $\overline{d/\nu(\delta)}$ is the gcd of the $\overline{a_i}$'s.

If for any i, $s_i' \leq s_i$, the existence of λ is obvious: $\lambda = \overline{q}$ answers the question. But it is not any more so obvious when there is one i for which $s_i' > s_i$. A fundamental idea to refer to and that we use many other times in this paper is to prove a property for d a power of prime ($d = p^s$) and then deduce that it is true for any composite d as in (118). This idea is achieved by the so-called Chinese remainder theorem.

Theorem 11 (Chinese remainder) *If $d = \prod_{i=1}^{n} p_i^{s_i}$ is the prime factor decomposition of d, then we have the following isomorphism of rings:*

$$\begin{array}{rccc} \pi: & \mathbb{Z}/d\mathbb{Z} & \xrightarrow{\sim} & \prod_{i=1}^{n} \mathbb{Z}/p_i^{s_i}\mathbb{Z} \\ & \overline{a} & \longmapsto & (a_1, \ldots, a_n) \end{array} \tag{121}$$

where $a_i = \pi_{p_i}(\overline{a})$ is the residue class of a modulo $p_i^{s_i}$. Addition and multiplication on the right-hand side of (121) are componentwise:

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n), \tag{122a}$$
$$(a_1, \ldots, a_n)(b_1, \ldots, b_n) = (a_1 b_1, \ldots, a_n b_n). \tag{122b}$$

The $\mathbb{Z}/p_i^{s_i}\mathbb{Z}$ in the theorem are called the Chinese factors of $\mathbb{Z}/d\mathbb{Z}$. According to (122b), a is invertible iff all its Chinese components a_i are. Thus, to solve our problem, we can equivalently search for a λ_i in each Chinese factor such that $a_i = \lambda_i x_i$. Moreover, we are going to give a first cumbersome proof of the existence of λ_i to show the necessity for the p-adic decomposition in each Chinese factor. Let us suppose that $d = p^s$, let $\nu = \nu(\overline{x}) = \nu(\overline{a})$ and suppose that both q and $q + \nu$ are noninvertible modulo d, that is to say p divides q and $q + \nu$. We are to prove this is impossible and thus there exists an invertible λ modulo d such that $\overline{a} = \overline{\lambda x}$. Indeed, since $a = qx$ and $p|q$ (p divides q) the properties $p^n|a$ and $p^{n-1}|x$ are true for $n = 1$.

Suppose they are true for some positive integer n. We know that $\overline{x}$ is a multiple of $\overline{a}$ in $\mathbb{Z}_d$ and thus there exist $k, l \in \mathbb{Z}$ such that $x = ka + ld = ka + l\nu x$. Since $p|(q+\nu) - q = \nu$ and $p^{n-1}|x$, $p^n|\nu x$ and then $p^n|x$ due to the induction hypothethis and to the previous expression for x. And since $p|q$ and $a = qx$, we deduce that $p^{n+1}|a$. Hence the property $p^n|a$ should be true for all positive integer n, what is clearly nonsense when $a \neq 0$. If $a = 0$, we can just replace it by d. We are now going to introduce the p-adic decomposition in $\mathbb{Z}/p^s\mathbb{Z}$ and compare with a proof using it.

Let a be a nonnegative integer and p be prime number. Writing a in numeration basis p, we get the numbers $r \in \mathbb{N}$ and $\alpha_0, \ldots, \alpha_r \in \{0, \ldots, p\}$ such that

$$a = \alpha_0 + \alpha_1 p + \cdots + \alpha_r p^r. \tag{123}$$

This is the p-adic decomposition of a. The p-valuation of a is

$$v_p(a) = \begin{cases} \min(i \in \{0, \ldots, r\}; \alpha_i \neq 0) \text{ for } a \neq 0, \\ +\infty \text{ for } a = 0. \end{cases} \tag{124}$$

For instance, if $a = \prod_{i=1}^n p_i^{s_i} \neq 0$ is the prime factor decomposition of a then for any $i \in \{1, \ldots, n\}$, $v_{p_i}(a) = s_i$.

Every class $\overline{a} \in \mathbb{Z}/p^s\mathbb{Z}$ is uniquely represented by an integer $a \in \{0, \ldots, p^s - 1\}$. So there exist one single $(\alpha_0, \ldots, \alpha_{s-1}) \in \{0, \ldots, p\}^s$ such that

$$\overline{a} = \alpha_0 \overline{1} + \alpha_1 \overline{p} + \cdots + \alpha_{s-1} \overline{p}^{s-1}. \tag{125}$$

This is the p-adic decomposition of $\overline{a}$. The p-valuation of $\overline{a}$ is

$$v_p(\overline{a}) = \begin{cases} \min(i \in \{0, \ldots, s-1\}; \alpha_i \neq 0) \text{ for } a \neq 0, \\ s \text{ for } a = 0. \end{cases} \tag{126}$$

The order of $\overline{a}$ is then $p^{s - v_p(\overline{a})}$ and $\overline{a}$ is invertible iff its valuation is 0. Moreover, for all $\overline{a}, \overline{b} \in \mathbb{Z}/p^s\mathbb{Z}$,

$$v_p(\overline{a} + \overline{b}) \geq \min(v_p(\overline{a}), v_p(\overline{b})), \tag{127a}$$
$$v_p(\overline{a}\overline{b}) = \min(v_p(\overline{a}) + v_p(\overline{b}), s), \tag{127b}$$

where equality in the latter formula relies on the fact that p is prime.

To check their understanding of p-adic decomposition, the reader should be able to see the following equalities, for any finite set $\{a_1, \ldots, a_n\} \subset \mathbb{Z}$ of divisors of some $d \geq 2$:

$$\left(\bigwedge_{i=1}^n a_i\right)\left(\bigvee_{i=1}^n d/a_i\right) = d, \tag{128a}$$
$$\left(\bigvee_{i=1}^n a_i\right)\left(\bigwedge_{i=1}^n d/a_i\right) = d. \tag{128b}$$

Now, let us hark back to our search for λ_i. Since they are of the same order, a_i and x_i are both zero or nonzero. If they are nonzero, then according to (127b) applied to $a_i = q_i x_i$, q_i is of p_i-valuation 0. Hence it is invertible in $\mathbb{Z}/p_i^{s_i}\mathbb{Z}$ and we take $\lambda_i = q_i$. If they are null, then $\nu_i = \pi_{p_i}(\overline{\nu}) = \overline{1}$ and either q_i or $q_i + \nu_i$ is of p_i-valuation 0 so that we get our λ_i. That is a simple proof of the

Lemma 12 *Let $d \geq 2$ and $a, b \in \mathbb{Z}_d$. The two following assertions are equivalent:*

1. *a, b are of the same order.*
2. *There exist $\lambda \in U(\mathbb{Z}_d)$ such that $a = \lambda b$.*

If one of them is satified, a and b are said to be associated. This is the case in particular if a and b are two gcd*'s of a same set of elements in $\mathbb{Z}_d$.*

What about the computation of the gcd of given $a_1, \ldots, a_m \in \mathbb{Z}/d\mathbb{Z}$ using the Chinese remainder theorem. Let $a_{ij} = \pi_{p_j}(a_i)$ for any $i \in \{1, \ldots, m\}$ and $j \in \{1, \ldots, n\}$. In order to lighten notations, we avoid the bar over residue classes in this paragraph. The set to which any element belongs will be known from the context. Let also $\delta = \bigwedge_{i=1}^m a_i$ in $\mathbb{Z}/d\mathbb{Z}$ and $\delta_j = \pi_{p_j}(\delta)$. It is quite obvious that in the j-th Chinese factor of $\mathbb{Z}/d\mathbb{Z}$ the gcd of the a_{ij}'s is

$$\bigwedge_{i=1}^{m} a_{ij} = p_j^{k_j}, \text{ with } k_j = \min(v_{p_j}(a_{ij}); i \in \{1, \ldots, m\}) \leq s_j. \tag{129}$$

Indeed, if i_0 is an index for which $v_{p_j}(a_{i_0 j}) = k_j$, then $a_{i_0 j} = p_j^{k_j} u$, where u is invertible. Thus $p_j^{k_j}$ may be obtained as a linear combination of the a_{ij}'s and any linear combination of them is a multiple of $p_j^{k_j}$. Moreover $p_j^{k_j} = p_j^{k_j} \wedge p_j^{s_j}$ in $\mathbb{Z}$. Since δ is a linear combination of the a_i's, δ_j is a linear combination of the a_{ij}'s and so $v_{p_j}(\delta_j) \geq k_j$. Then, a_{i_0} being a multiple of δ, $a_{i_0 j}$ is a multiple of δ_j and so $v_{p_j}(\delta_j) = k_j$. Hence $\delta = \prod_{j=1}^m p_j^{k_j}$. All this is nothing but the usual way to compute gcd's by means of prime factor decomposition.

Another useful lemma is the following one. It is not often found in literature maybe for the crux is easy to see.

Lemma 13 *Let $d \geq 2$ and $a, b, \delta \in \mathbb{Z}_d$ such that δ is a* gcd *for a and b. If one of the following conditions is verified:*

- *d is odd,*
- *d is even and $v_2(a) \neq v_2(b)$,*
- *d is even and $v_2(a) = v_2(b) = v_2(d)$;*

then one can choose $u, v \in U(\mathbb{Z}_d)$ such that $\delta = ua + vb$. If not, then only u or v can be chosen invertible.

Proof. In this proof, in order to distinguish classes and representatives, we shall note $\overline{a}, \overline{b}, \overline{\delta}$ instead of a, b, δ as in the terms of the lemma. Using the Chinese remainder theorem, we search for u and v in each Chinese factor separately. So suppose $d = p^s$, with p odd to begin with. Also note that owing to of lemma 12, it suffices to prove lemma 13 for any gcd $\overline{\delta}$ of $\overline{a}$ and $\overline{b}$. So we will choose $\delta = a \wedge b$, taking into account the remark just following (102). By definition, there exist $u_0, v_0 \in \mathbb{Z}$ such that $\delta = u_0 a + v_0 b$, and dividing by δ we obtain

$$1 = u_0 a' + v_0 b' \tag{130}$$

where $a' = a/\delta$, $b' = b/\delta$. We see that u_0 and v_0 cannot be both multiples of p. At least one of $\overline{u_0}$ and $\overline{v_0}$, say $\overline{u_0}$, is a unit. Suppose $\overline{v_0}$ is not a unit, that is to say v_0 is a multiple of p. If $v_0 + a'$ were a multiple of p, then so would a', what would contradict (130) once more. So $v_0 + a'$ is a unit and so is $v_0 - a'$. Besides, if $u_0 \pm b'$ were both mutiples of p, so would be $2b'$, b' and then u_0. We may now conclude that at least one of the three pairs

$$(\overline{u_0}, \overline{v_0}),\ (\overline{u_0 + b'}, \overline{v_0 - a'}) \text{ and } (\overline{u_0 - b'}, \overline{v_0 + a'}) \tag{131}$$

is in $U(\mathbb{Z}_d)^2$. That proves the lemma as to the first condition.

If $p = 2$ and $v_2(\overline{a}) \neq v_2(\overline{b})$, then in (130), one of a' and b' is odd, say a', and the other is even, say b'. Moreover, u_0 has to be odd too. Then one of the two pairs

$$(\overline{u_0}, \overline{v_0}) \text{ and } (\overline{u_0 + b'}, \overline{v_0 - a'}) \tag{132}$$

is in $U(\mathbb{Z}_d)^2$.

If $p = 2$ and $v_2(\overline{a}) = v_2(\overline{b}) = v_2(d)$, then $\overline{a} = \overline{b} = \overline{\delta} = 0$ and $u = v = 1$ suit the lemma.

Still with $p = 2$, if $v_2(\overline{a}) = v_2(\overline{b}) \neq v_2(d)$, we have already seen that at least one of $\overline{u_0}$ and $\overline{v_0}$, say $\overline{u_0}$, is a unit. But $\overline{v_0}$ cannot be a unit, since in that case $u_0 a' + v_0 b'$ should be even. Because we only need $u_0 a' + v_0 b'$ to be odd, we can choose which one of $\overline{u_0}$ and $\overline{v_0}$ is invertible. ■

By induction and associativity of gcd, we have the

Corollary 14 *Let $a_1, a_2, \ldots, a_n \in \mathbb{Z}_d$ and δ be one of their* gcd*'s. For any $i \in \{1, \ldots, n\}$, one can find $k_1, k_2, \ldots, k_n \in \mathbb{Z}_d$ with $k_i \in U(\mathbb{Z}_d)$ such that*

$$\delta = \sum_{j=1}^{n} k_j a_j. \tag{133}$$

Appendix B Finitely generated modules over $\mathbb{Z}_d$

Let d and n be two positive integers with $d \geq 2$. The set product $\mathbb{Z}_d^n$ is endowed with its canonical structure of $\mathbb{Z}$-module and its elements will be called vectors. Addition is componentwise:

$$\begin{array}{rcl} \mathbb{Z}_d^n \times \mathbb{Z}_d^n & \longrightarrow & \mathbb{Z}_d^n \\ ((a_1, \ldots, a_n), (b_1, \ldots, b_n)) & \longmapsto & (a_1 + b_1, \ldots, a_n + b_n) \end{array} \tag{134}$$

and the product map is

$$\begin{array}{rcl} \mathbb{Z} \times \mathbb{Z}_d^n & \longrightarrow & \mathbb{Z}_d^n \\ (k,(a_1,\ldots,a_n)) & \longmapsto & (ka_1,\ldots,ka_n). \end{array} \tag{135}$$

This can also be denoted $k \cdot (a_1,\ldots,a_n)$ or even $k(a_1,\ldots,a_n)$ without a symbol. Obviously, such a product depends only on the residue class of k modulo d, so that we may consider $\mathbb{Z}_d^n$ either as a $\mathbb{Z}$-module or a $\mathbb{Z}_d$-module. So, when the context is clear or the distinction useless, one can avoid the bar to denote residue classes.

A submodule of $\mathbb{Z}_d^n$ is a module over $\mathbb{Z}_d$ included in $\mathbb{Z}_d^n$. When $n = 1$, submodules are called ideals of $\mathbb{Z}_d$. Let I be a finite index set and $m = (m_i)_{i\in I}$ be a family of vectors in $\mathbb{Z}_d^n$. The submodule those vectors generate is the set of all their linear combinations over $\mathbb{Z}_d$ and is noted $\langle m\rangle$, or $\langle m_1,\ldots,m_r\rangle$ whenever $I = \{1,\ldots,r\}$. It is the tiniest submodule that contains all the m_i's. The family m is a generating system or basis of that submodule. Moreover, any submodule of $\mathbb{Z}_d^n$ is generated by some basis, since the whole submodule itself is such a basis. The family m is free if for all family $(c_i)_{i\in I}$ of elements of $\mathbb{Z}_d$,

$$\sum_{i\in I} c_i m_i = 0 \Longrightarrow \forall i \in I, c_i = 0. \tag{136}$$

In other words, the linear map

$$\begin{array}{rrcl} f_m : & \mathbb{Z}_d^I & \longrightarrow & \mathbb{Z}_d^n \\ & (c_i)_{i\in I} & \longmapsto & \sum_{i\in I} c_i m_i \end{array} \tag{137}$$

has kernel 0. A basis of a submodule which is also free is called a free basis of that submodule, and a submodule for which there exists a free basis is called a free submodule. The computational basis of $\mathbb{Z}_d^n$ is of course a free basis and it will be denoted by $e = (e_i)_{i=1\ldots n}$. For any vector a, $e_i^*(a) = a_i$ is the i-th component of a with respect to e.

A vector a such that the one-element family (a) is free is called a free vector. If moreover $n = 1$, then a is just said regular.

A submodule M is said to be of rank r if the minimal number of vectors needed to generate it is r. This notion of rank should not be confused with the rank of the matrix whose columns are a set of generating vectors of M with respect to some free basis of $\mathbb{Z}_d^n$ (see [36]). Those two notions of rank for submodules and matrices do not overlap.

A minimal basis for a rank-r submodule M is a basis of M with r elements. Such a basis need not be free. For instance in $\mathbb{Z}_4^2$, $((2,0))$ is a basis for the rank-1 submodule $\{(0,0),(2,0)\}$ but is not free. But if M is free, minimal and free bases are the same ones. Indeed, let $(m_i)_{i=1,\ldots,r}$ be a minimal basis of M and $(m'_i)_{i\in I}$ be a free basis of M. By minimality of m, $r \le |I|$ and by freedom of m', $|\mathrm{Im}\, f_{m'}| = d^{|I|}$. So

$$|M| = |\mathrm{Im}\, f_m| \le d^r \le d^{|I|} = |\mathrm{Im}\, f_{m'}| = |M|\,. \tag{138}$$

Thus on the one hand $|\mathrm{Im}\, f_m| = d^r$ and f_m must be injective, so that m is free. On the other hand, $|I| = r$ implies that m' is minimal.

Let $a = (a_1, \ldots, a_n) \in \mathbb{Z}_d^n$. The order $\nu(a)$ of a is the cardinality of the set $\mathbb{Z}_d \cdot a = \{ka; k \in \mathbb{Z}_d\}$. The only vector whose order is 1 is the null vector and a is a free vector iff $\nu(a) = d$. Endly, we note that $\nu(a)\mathbb{Z}$ is the kernel of the linear map

$$\begin{array}{rccc} f: & \mathbb{Z} & \longrightarrow & \mathbb{Z}_d^n \\ & k & \longmapsto & ka. \end{array} \tag{139}$$

This kernel is the intersection of the $\ker(e_i^* \circ f) = \nu(a_i)\mathbb{Z}$ and thus

$$\nu(a) = \bigvee_{i=1}^{n} \nu(a_i). \tag{140}$$

With (117) and (128a) we also deduce that

$$\nu(a) = \frac{d}{(\bigwedge_{i=1}^{n} a_i) \wedge d}. \tag{141}$$

References

[1] C. H. Bennett and G. Brassard. In *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, pages 175–179. Bangalore, India (IEEE, New York), 1984.

[2] P. W. Shor. Algorithms for quantum computation: discrete logarithm and factoring. In S. Goldwasser, editor, *Proceedings of the 35th. Annual Symposium on the Fonudations of Computers Science*, page 124. IEEE Computer Society Press, Los Alamitos, CA, 1994.

[3] J. Schwinger. Unitary operators bases. In *Proceedings of the National Academy of Sciences*, volume 46, pages 570–579, 1960.

[4] W. K. Wootters and B. D. Fields. Optimal state-determination by mutually unbiased measurements. *Annals of Physics*, 191:363–381, 1989.

[5] L. Vaidman, Y. Aharonov, and D. Z. Albert. How to ascertain values of σ_x, σ_y, and σ_z of a spin-$\frac{1}{2}$ particle. *Physical Review Letters*, 58(14):1385–1387, 1987.

[6] A. Hayashi, M. Horibe, and T. Hashimoto. Mean king's problem with mutually unbiased bases and orthogonal latin squares. *Physical Review A*, 71:052331, 2005.

[7] J. P. Paz, A. J. Roncaglia, and M. Saraceno. Qubits in phase space: Wigner function approach to quantum error correction and the mean king problem. *Physical Review A*, 72:012309, 2005.

[8] A. R. Calderbank, P. J. Cameron, W. M. Kantor, and J. J. Seidel. $\mathbb{Z}_4$-Kerdock codes, orthogonal spreads, and extremal euclidean line-sets. In *Proceedings of the London Mathematical Society*, volume 75, pages 436–480, 1997.

[9] J. M. Renes. *Frames, designs, and spherical codes in quantum information theory.* PhD thesis, University of New Mexico, Albuquerque, New Mexico, 2004. Dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy Physics, http://kerr.physik.uni-erlangen.de/ renes/publications/diss2side.pdf.

[10] J. M. Renes. Optimal protocols and tradeoffs in quantum key distribution. In *AIP Conference Proceedings*, 2004.

[11] R. W. Heath, T. Strohmer, and A. J. Paulraj. On quasi-orthogonal signatures for CDMA systems. *IEEE Transactions on Information Theory*, 52(3):1217–1226, 2006.

[12] I. D. Ivanović. Geometrical description of quantal state determination. *Journal of Physics A*, 14:3241–3245, 1981.

[13] A. Klappenecker and M. Rtteler. Constructions of mutually unbiased bases. In *Proceedings International Conference on Finite Fields and Applications*, volume 2948, pages 137–144. LNCS, Springer, 2004.

[14] C. Archer. There is no generalization of known formulas for mutually unbiased bases. *Journal of Mathematical Physics*, 46:022106, 2005.

[15] S. Bandyopadhyay, P. O. Boykin, V. Roychowdhury, and F. Vatan. A new proof for the existence of mutually unbiased bases. *Algorithmica*, 34:512–528, 2002.

[16] W. K. Wootters. Quantum measurements and finite geometry. *Foundations of Physics*, 36:112, 2006.

[17] A. Vourdas. Galois quantum systems. *Journal of Physics A*, 38:8453–8471, 2005.

[18] E. F. Galvão. Discrete Wigner functions and quantum computational speedup. *Physical Review A*, 71:042302, 2005.

[19] A. O. Pittenger and M. H. Rubin. Wigner functions and separability for finite systems. *Journal of Physics A*, 38:6005–6036, 2005.

[20] A. B. Klimov, L. L. Sánchez-Soto, and H. de Guise. A complementary-based approach to phase in finite-dimensional quantum systems. *Journal of Optics B*, 7:283–287, 2005.

[21] A. B. Klimov, L. L. Sánchez-Soto, and H. de Guise. Multicomplementary operators via finite Fourier transform. *Journal of Physics A*, 38:2747–2760, 2005.

[22] M. Saniga, M. Planat, and H. Rosu. Mutually unbiased bases and finite projective planes. *Journal of Optics B*, 6:L19–20, 2004.

[23] M. Saniga and M. Planat. Sets of Mutually Unbiased Bases as Arcs in Finite Projective Planes? *Chaos, Solitons and Fractals*, 26:1267 – 1270, 2005.

[24] M. Planat, H. Rosu, S. Perrine, and M. Saniga. A Survey of Finite Algebraic Geometrical Structures Underlying Mutually Unbiased Quantum Measurements. *Foundations of Physics*, 36:1662–1680, 2006.

[25] M. Kibler. Angular momentum and mutually unbiased bases. *International Journal of Modern Physics B*, 20(11-13):1792–1801, 2006.

[26] M. Kibler and M. Planat. A $SU(2)$ recipe for mutually unbiased bases. *International Journal of Modern Physics B*, 20(11-13):1802–1807, 2006.

[27] O. Albouy and M. Kibler. $SU(2)$ Nonstandard Bases: Case of Mutually Unbiased Bases. *Symmetry, Integrability and Geometry: Methods and Applications*, 3:076, 2007.

[28] O. Albouy and M. Kibler. A unified approach to SIC-POVMs and MUBs. *Journal of Russian Laser Research*, 28(5), 2007.

[29] M. Planat, M. Saniga, and Kibler M. Quantum Entanglement and Projective Ring Geometry. *Symmetry, Integrability and Geometry: Methods and Applications*, 2:066, 2006.

[30] R. Howe. Nice error bases, mutually unbiased bases, induced representations, the Heisenberg group and finite geometries. *Indag. Mathem., N.S.*, 16(3-4):553–583, 2005.

[31] M. Kibler. Variations on a theme of Heisenberg, Pauli and Weyl. *Journal of Physics A*, 41:375302, 2008.

[32] M. Planat and M. Saniga. On the Pauli graphs of N-qudits. *Quantum Information and Computation*, 8(1-2):127–146, 2008.

[33] M. Planat and M. Saniga. Qudits of composite dimension, mutually unbiased bases and projective ring geometry. *Journal of Physics A*, 40:F1–F8, 2007.

[34] H. Havlicek and M. Saniga. Projective Ring Line of a Specific Qudit. *Journal of Physics A*, 40:F943–F952, 2007.

[35] H. Havlicek and M. Saniga. Projective Ring Line of an Arbitrary Single Qudit. *Journal of Physics A*, 41:015302, 2008.

[36] William C. Brown. *Matrices over commutative rings*. Pure and applied mathematics. Marcel Dekker, Inc., 1993.

[37] I. Kaplansky. Elementary divisors and modules. *Transactions of the American Mathematical Society*, 66:464–491, 1949.

[38] Max D. Larsen, William J. Lewis, and Thomas S. Shores. Elementary divisor rings and finitely presented modules. *Transactions of the American Mathematical Society*, 187(1):231–248, 1974.